UNIVERSIDAD DE CHILE
FACULTAD DE DERECHO
DEPARTAMENTO DE DERECHO PROCESAL
CENTRO DE ESTUDIOS EN DERECHO INFORMÁTICO

WIKILEAKS ANTE EL DERECHO ESTADOUNIDENSE: ¿DELINCUENCIA INFORMÁTICA, ESPIONAJE O EJERCICIO LEGÍTIMO DE LA LIBERTAD DE EXPRESIÓN Y DE PRENSA?

Memoria de prueba para optar al grado de Licenciado en Ciencias Jurídicas y Sociales

---

FELIPE GONZALO CAMPOS ARLEGUI

Profesor Guía Dr. Salvador Andrés Millaleo Hernández

Santiago de Chile
2014

A mi familia, pero por sobretodo y por siempre a mi madre.

TABLA DE CONTENIDOS

INTRODUCCIÓN

La así llamada “experiencia *WikiLeaks*” nos ha hecho reflexionar acerca de la extensión de la libertad de expresión y de prensa en Estados Unidos, dado que se trata de una nación fundada en ella y su líder durante el transcurso de toda su historia. Además, esa nación devino la principal potencia comunicativa, influyendo y determinando la construcción cultural del occidente post Segunda Guerra, sin olvidar que se trata de la primera potencia económica y militar de La Tierra indiscutiblemente desde el fin de la guerra fría. Con sólo esos hechos se demuestra el interés de allegar antecedentes a la reflexión.

La historia ha seguido avanzando y lo anterior debemos contextualizarlo con el desarrollo actual y acelerado de las nuevas tecnologías de la información, que además, se encuentran en una fase de acceso incomparablemente más fácil, económico y en consecuencia, generalizado de lo que era hace sólo algunos años atrás para los ciudadanos de nivel económico medio de los países del primer y tercer mundo occidental. Ello, naturalmente nos induce a tratar de responder a las también nuevas preguntas que han emergido tanto en el desarrollo general del estudio de las nuevas tecnologías, como en la pregunta específica que surge desde esta memoria de grado: ¿Los actos de *WikiLeaks* son conductas de delincuencia informática, de espionaje o es ejercicio legítimo de la libertad de expresión y de prensa ante el derecho estadounidense?

Para ordenar los factores más determinantes que responderán esta pregunta hemos establecido tres capítulos. Ellos buscarán ir acercándose paulatinamente a la respuesta avanzando a través de párrafos que generan subpreguntas, naturalmente entregándose reflexiones desde las fuentes más

autorizadas, algunas respondidas en el mismo capítulo en el que se ofrecieron, otras reservadas su respuesta para la parte conclusiva de este trabajo.

De esta manera, el primer capítulo se hace cargo de las primeras preguntas de la experiencia *WikiLeaks*: ¿Qué es un sitio *wiki*? ¿Qué es el *leaking*? ¿Cómo se origina y estructura *WikiLeaks*? Todo ello para acercarnos a un conocimiento y entendimiento al de qué estamos hablando cuando hablamos de *WikiLeaks*, buscando la existencia de precedentes organizacionales, estableciendo el contexto que posibilita su aparición y exponiendo sus elementos estructurales fundamentales y sus primeras acciones para comenzar a dilucidar la respuesta a la pregunta de tesis.

Luego, en el segundo capítulo, decidimos profundizar de manera mucho más detallada en aquellas filtraciones que han generado mayor interés en el periodismo, en la opinión pública, interés y reacciones del gobierno norteamericano y preguntas y reflexión en su doctrina. Ellas son las del video asesinato colateral, los diarios de guerra de Afganistán, los documentos de Irak y la filtración de los cables diplomáticos, esta última, implicante de la reacción de los Estados Unidos.

Finalmente el tercer y último capítulo, el más extenso, intentará, habiéndonos hecho cargo de las preguntas anteriores, agregar antecedentes tanto sobre la reacción de las autoridades norteamericanas, tanto sobre aquello que plantea la Primera Enmienda y las leyes que según la doctrina podrían invocarse por parte de los persecutores, allegar los precedentes judiciales que según la doctrina especializada serían los más atingentes para estudiar una posible decisión jurisdiccional al eventual procesamiento de Assange, y finalmente, exponer las opiniones de los estudiosos más autorizados.

Es importante advertir al lector que la presente investigación si bien plantea el análisis de leyes penales, dada la naturaleza del tema de

investigación situamos mayormente nuestro interés en el estudio de su aplicabilidad determinada por razonamientos en sede constitucional y que, finalmente, lo buscado es aportar con antecedentes y con reflexiones a las posibles discusiones sin tener la pretensión de agotarla.

CAPÍTULO I

¿QUÉ ES UN SITIO *WIKI*? ¿QUÉ ES EL *LEAKING*? ¿QUIÉN ES EL FUNDADOR Y LOS PRINCIPALES COLABORADORES DE *WIKILEAKS*? ¿CUÁL ES SU BASE TECNOLÓGICA? ¿CUÁLES SON SUS PRIMERAS FILTRACIONES?

I.1. ¿QUÉ ES UN SITIO *WIKI*?

La primera pregunta que emerge es la que exige como respuesta la de dilucidar los elementos que estructuran un sitio *Wiki* y que lo distinguen de cualquier otro tipo de sitio en la Internet. ¿Por qué surge esta pregunta antes que cualquier otra? Porque uno de los objetivos centrales de este trabajo es el de establecer de qué hablamos cuando hablamos de *WikiLeaks*, y el primer elemento a desentrañar es justamente el de su denominación.

I.1.1. Los primeros Wiki.

I.1.1.1. WikiWikiWeb[1]*.* Fue abierto a la Internet por su fundador, Ward Cunningham[2], el 25 de marzo de 1995. ¿Por qué le dio una designación nueva a su sitio? En primer lugar, porque se trataba de una creación, y en segundo lugar, posiblemente quiso contraponer el divertido nombre *WikiWikiWeb* a la ya en esos años repetida designación para llamar a la red de redes *Worldwide Web.* ¿Por qué se decidió finalmente por la distintiva palabra "*Wiki*" como componente del nombre de su sitio? *Wiki* es una palabra de origen hawaiano

[1] [en línea] <c2.com/cgi/wiki?WikiWikiWeb> [Consulta: 08/09/2012]
[2] Ingeniero interdisciplinario en electricidad y en computación, con una maestría en ciencias de la computación. [en línea] <es.wikipedia.org/wiki/Ward_Cunningham> [Consulta: 08/09/2012]

que significa “rápido”, en contraste a la lentitud de que adolecen los formatos tradicionales para entregar nuevas ediciones, más actualizadas y perfeccionadas. Ello, junto al carácter colaborativo o social de la edición, conforman el núcleo que de lo que entenderemos por sitio *wiki*. ¿Qué realiza concretamente el sitio? El sitio hace posible la interacción entre programadores para exponer sus diseños a la comunidad, ir mejorando las obras colectivamente y compartir los resultados.

I.1.1.2. Wikipedia[3]*.* Inspirados, por las ambiciones perseguidas por la Biblioteca de Alejandría de reunir sistemáticamente todo el conocimiento humano[4], por el sueño de conformar una expresión que permitiera la existencia de un sistema social más justo y equitativo y además por el entusiasmo que seguramente les produjo la rapidez y socialización de edición y de beneficios del formato, Jimmy Wales[5] junto a Larry Sander[6] decidieron utilizar un *wiki* como base para el proyecto de enciclopedia *Wikipedia e*n enero de 2001.

Esta biblioteca en línea es uno de los diez sitios *web* más populares del mundo, la primera enciclopedia doblada a 282 lenguas, que ofrece casi veinte millones de artículos en total sobre ciencia, arte, tecnología, historia y otros tantos campos del saber.

[3] [en línea] <wikipedia.org/> [Consulta: 08/09/2012]
[4] [en línea] <en.wikipedia.org/wiki/Wikipedia:Wikipedia_Signpost/2010-05-10/Book_review> [Consulta: 08/09/2012]
[5] Licenciado y candidato a Doctor en Finanzas. [en línea] <es.wikipedia.org/wiki/Jimmy_Wales> [Consulta: 08/09/2012]
[6] Filósofo. [en línea] <http://es.wikipedia.org/wiki/Larry_Sanger> [Consulta: 08/09/2012]

Solicitar información dentro del sitio es muy sencillo y rápido, al igual que editar sus contenidos. Se sostiene sobre la idea de que el conocimiento es obra de la colectividad por lo tanto la colectividad debe tener acceso sin restricciones al fruto de su propia interacción. De ahí el nombre de Wikipedia, "*wiki*" de rápido, "*pedia*" de conocimiento.

I.1.2 ¿Cuáles son los elementos esenciales de un Wiki?

Para Brian Lamb[7], es arriesgado hablar de *wikis* como si fueran todos iguales. Se aplica este término a un conjunto diverso de sistemas y proyectos. Sin embargo, algunas características fundamentales se pueden extraer de ellos[8]:

I.1.2.1. Autoría colectiva. Los *wiki* son rápidos porque los procesos de lectura y edición son similares. Un enlace en la página que estamos leyendo nos permite editarla: escribir, corregir, reescribir o suprimir un texto. El *wiki* típico, está abierto a las aportaciones e intervenciones de cualquier persona que lo desee. *Softwares* de autoría, de permisos o contraseñas no suelen ser necesarios.

I.1.2.2. Limitado uso del HTML y uso de una estructura hipertextual. La producción de textos está enmarcada en un contexto muy simple, en concordancia con la rapidez de que se busca dotar al sitio, pero a cambio, renunciando al uso de herramientas de diseño o multimediales que hagan de la experiencia algo más integral. Además, en contraposición a la estructura lineal de libros y documentos en formato pdf, existe una página principal a la que se accede por defecto, y desde allí, se podrá acceder libremente a los distintos contenidos a través de los enlaces de hipertexto.

[7] Coordinador de proyectos de la Oficina de Tecnología Educativa de la Universidad de British Columbia.
[8] LAMB, Brian. "*Wide Open Spaces: Wikis, Ready or Not*". [Amplios Espacios Abiertos: Wikis, Listo o No]. Educause Review, vol. 39, no. 5 (September/October 2004): 36–48. [en línea] <www.educause.edu/ero/article/wide-open-spaces-wikis-ready-or-not> [Consulta: 10/09/2012]

I.1.2.3. Flexibilidad. Un *wiki* no tiene una estructura predefinida, cualquiera puede crear nuevas páginas y vincularlas a cualquier otra. Es tan flexible en su estructura, que sin cierta labor de edición y algunas normas puede devenir en un caos rápidamente. Pero al mismo tiempo, su flexibilidad permite la construcción colaborativa y progresiva de espacios hipertextuales complejos de información.

I.1.2.4. Están libres de ego, libres de tiempo y nunca acabados. El anonimato no es obligatorio, pero es común. Con su edición abierta, puede tener múltiples contribuyentes, y las nociones de "autoría" y "propiedad" pueden verse radicalmente alteradas. A diferencia de los *weblogs*, raramente son organizados cronológicamente, se organizan por el contexto, por vínculos y enlaces hacia fuera, y por las categorías o conceptos que surjan en el proceso de creación. Las entradas están a menudo sin pulir, y los creadores deliberadamente dejan espacios abiertos, con la esperanza de que alguien más va a venir a llenarlos. Los *wiki* están en un estado constante de flujo. Por ello la recomendación de que al citarse una página de Internet debe indicarse la fecha de su visita, adquiere mayor vigor cuando se trata de un sitio de este tipo.

I.1.3. ¿Qué otro elemento diferenciador no esencial hay en un wiki?

Motivados por el éxito de *Wikipedia*, los *wiki* han recibido bastante atención desde la investigación social. Ebersbach y Glaser[9], por ejemplo, analizaron si los *wiki* y la filosofía *wiki* cumplen los criterios que en 1970 Enzensberger[10] impuso al uso emancipatorio de un medio[11]: ¿Qué es el uso emancipatorio de un medio? Está dado por el cumplimiento de las siguientes exigencias: Descentralización; Cada receptor puede ser un emisor potencial; Movilización de masas; Producción colectiva; Interacción de los participantes; Control social mediante la autoorganización, y; Procesos de aprendizaje político.

[9] EBERSBACH, Anja y Glaser, Markus. *"Towards Emancipatory Use of a Medium: The Wiki"*. [Hacia un uso emancipador de un medio: El Wiki]. International Journal of Information Ethics, Vol. 2 (11/2004) [en línea] <http://fiz1.fh-potsdam.de/volltext/ijie/05250.pdf> [Consulta: 12/09/2012]

[10] *"Constituents of a Theory of the Media"*. [Componentes de una Teoría de los Medios de Comunicación]. New Left Review, no. 64, 1970, pp. 13-36.

[11] Según QUESADA, Rocío. *"La didáctica crítica y la tecnología educativa"* Revista Perfiles Educativos de la Universidad Nacional Autónoma de México, No. 49 – 50 pp. 3 – 13. 1990. [en línea] <http://132.248.192.201/seccion/perfiles/1990/n49-50a1990/mx.peredu.1990.n49-50.p3-13.pdf>
[Consulta: 12/09/2012] El teórico crítico Jürgen Habermas habla de "interés emancipatorio", el cual nos puede ser muy útil para aclararnos de qué se trata el "uso emancipatorio" de un medio. Al "interés emancipatorio" se llega desde que según él la ciencia y el saber obedecen a los intereses particulares a los que sirven, y desde allí desprende el concepto de "los intereses constitutivos de saberes" que son tres: el "técnico", el "práctico" y el "emancipatorio".
1.- El interés técnico: es aquel motivado por adquirir conocimientos que faciliten un control técnico sobre los objetos naturales. Produce buena parte de los saberes necesarios para la industria y los sistemas de producción. Por lo tanto su saber es instrumental, el medio utilizado para su consecución es el trabajo y las ciencias que lo determinan son las empírico – analíticas o naturales. CARR Wilfred, Kemmis Stephen. *"Teoría crítica de la enseñanza"*. 1988, p. 148.
2.- El interés práctico: clarifica la comunicación significativa y "genera conocimiento en forma de entendimiento interpretativo capaz de informar y de guiar el juicio práctico". Su saber es eminentemente práctico, el medio para conseguir sus finalidad es el lenguaje y sus ciencias son las hermenéuticas o interpretativas. CARR Wilfred, op. cit., p. 148.
3.- El interés emancipador: exige que se superen las preocupaciones estrechas para con los significados subjetivos "a fin de alcanzar un conocimiento emancipador acerca del marco de referencia objetivo en el que pueden producirse la comunicación y la acción social. De ese conocimiento objetivo quiere ocuparse esencialmente la ciencia social crítica." Su saber es emancipatorio – reflexivo, su medio es el poder y sus ciencias son las ciencias críticas. idem, p. 148 - 149.
Una de las misiones de la ciencia social crítica es aquella que "yendo más allá de la crítica aborde la praxis crítica; esto es, una forma de práctica en la que la ilustración de los agentes tenga su consecuencia directa en una acción social transformada. Esto requiere una integración de la teoría y la práctica en momentos reflexivos y prácticos de un proceso dialéctico de reflexión, ilustración y lucha política llevada a cabo por los grupos con el objetivo de su propia emancipación". ". Idem, p. 157.
De esta manera podemos entender como uso emancipatorio de un medio, aquel que a través del interés emancipatorio ya descrito, crea conocimiento emancipador, esto es, el uso de un medio educando o informando para la acción social y la lucha política cuyo fin es el de emancipar a los propios receptores.

Impresiona que Enzensberger escribiera acerca de las condiciones de un medio para que se considerase de uso emancipatorio hace 43 años, anticipándose al desarrollo de la Internet y, en especial, de los *wiki*, siendo justamente este tipo de página *web*, la que incluso abre una nueva etapa en el desarrollo de la *World Wide Web*, la *web* 2.0, y siendo también la que cumple de mejor manera con aquellas condiciones.

"Hoy en día, el conflicto sobre los derechos digitales y el acceso gratuito a la información desempeña un papel fundamental, la participación en un *wiki*, y en especial en *Wikipedia*, también es una decisión voluntaria, de tomar partido en favor de la libertad de información. Este es un acto político, que está afectando al mundo real, manteniendo algo más de información en la esfera pública."[12]

Desde este punto, podemos decir que un medio o nueva tecnología no sólo puede conceptualizarse desde los avances y diferencias tecnológicas que aportan sino que también desde su filosofía y expresión social, y es así como para nosotros, un importante elemento diferenciador en la conceptualización misma de un *wiki* es el de que debe estar dotado de un uso emancipatorio.

I.1.4. ¿Cuál es nuestro concepto de Wiki?

Después de haber revisado brevemente la historia de los precursores de la filosofía y tecnología *wiki* y de determinar los elementos que configuran y diferencian a un sitio *wiki*, bien podríamos encontrarnos en el punto de poder darnos la posibilidad de armar nuestro propio concepto de lo que es, no sin antes hacer mención a conceptualizaciones anteriores que pueden ayudarnos a lograr lo que buscamos.

[12] EBERSBACH y Glaser, op cit., p.8.

I.1.4.1. Concepto del fundador de WikiWikiWeb. En palabras del propio Cunningham, un *wiki* es "la base de datos en línea más simple que pueda funcionar". Este concepto atiende a la simpleza e indirectamente a la rapidez, este último uno de los aspectos característicos de un *wiki,* precisamente el que le dio el nombre, pero no se hace cargo de otros aspectos igualmente importantes.

I.1.4.2. Concepto del Oxford English Dictionary. La palabra *wiki* deja paso a su significado en hawaiano para construir un nuevo significado en inglés: "un tipo de página *web* diseñada de forma tal que sus contenidos puedan ser editados por cualquier persona que acceda a ella.[13]" Este concepto se basa en la autoría social, pero deja de lado la simpleza y sobretodo la rapidez del concepto del creador de los *wikis*.

I.1.4.3. Concepto de Oxforddictionaries.com/. "un sitio *web* o base de datos desarrollada colaborativamente por una comunidad de usuarios, permitiéndose a cualquiera de ellos añadir y editar contenido.[14]" Desarrolla mejor que el anterior el punto de la autoría colectiva pero también adolece de incompletitud al desestimar otros aspectos también esenciales.

I.1.4.4. Nuestro concepto. Para nosotros, un *wiki* es "el sitio *web* o base de datos que otorga a toda su comunidad de usuarios herramientas tecnológicas de rápido aprendizaje y fácil ejecución, para que mediante la colaboración colectiva y su uso emancipatorio se genere información y conocimiento disponible para todos."

[13] REUTERS, *"Wiki wins a place in Oxford English Dictionary"*. [Wiki gana un lugar en el Diccionario Oxford de Inglés]. 15 de Marzo de 2007, [en línea] <http://www.reuters.com/article/2007/03/15/us-britain-dictionary-wiki-idUSL1528182320070315> [Consulta: 10/09/2012]
[14] [en línea] <http://oxforddictionaries.com/es/definicion/ingles/wiki> [Consulta: 10/09/2012]

WikiLeaks comenzó como un *wiki*, pudiendo ser modificada por los usuarios. Pero Assange y sus colegas se dieron cuenta de que el contenido y la necesidad de eliminar información peligrosa o comprometedora convertían ese modelo en impracticable. Pero aunque los elementos *wiki* de edición social habían sido abandonados, en el corazón del concepto de *WikiLeaks* permanece una estructura que permite la presentación anónima de documentos filtrados para la elaboración de una reflexión social emancipatoria.[15]

I.2. ¿QUÉ ES EL *LEAKING*?

Para seguir nuestra investigación en relación a qué decimos cuando hablamos de *WikiLeaks*, explicando su propia denominación y el por qué de su elección, naturalmente lo que nos queda es hacernos cargo de responder a la pregunta ¿Qué es el *leaking*?

Para ello recurriremos a la misma metodología que en el apartado anterior, es decir, haremos mención de la existencia de precedentes, dos también en este caso, uno más vinculado a la historia y el otro a la tecnología, luego dilucidaremos los elementos esenciales de un *leaking* y finalmente establecemos nuestro propio concepto de este dentro del contexto que nos interesa.

I.2.1. Precedentes. Los Pentagon papers y Cryptome.org.

[15] LEIGH, David y Harding, Luke. *"Wikileaks: Inside Julian Assange´s War on Secrecy"*. [Wikileaks: Dentro de la guerra de Julian Assange en secreto]. Guardian books, traducción de Mar Vidal e Isabel Merino bajo el título:*"Wikileaks y Assange. Un relato trepidante sobre cómo se fraguó la mayor filtración de la historia"*, Ediciones Deusto, Barcelona, 2011, p. 68.

I.2.1.1. El precedente histórico: Los Pentagon Papers. Daniel Ellsberg, nacido en 1931 en Detroit, graduado de Harvard, destacó en Ciencia Política y Economía. Fue un investigador, analista, además de un brillante teórico en Ciencias Políticas que colaboró académicamente con un entonces desconocido Henry Kissinger.[16]

En 1964 comenzó a trabajar en el Pentágono, justamente cuando comenzaba la implicación estadounidense en Vietnam. De hecho, comenzó su trabajo el 4 de Agosto, día del segundo incidente del Golfo de Tonkín, suceso que luego él mismo comprobaría falso, pero que fue utilizado por la administración Johnson como excusa para atacar a Vietnam del Norte.[17]

En un comienzo, Ellsberg fue uno de los "arquitectos de la guerra", siendo parte de un equipo de analistas que trabajaban estrechamente con el Pentágono redactando informes, elaborando planes bélicos y realizando estadísticas.[18]

[16] SANCHEZ, Carlos. *"Analogías de la Historia I: Julian Assange y Wikileaks vs Daniel Ellsberg y los Pentagon Papers"*. Nómadas. Revista Crítica de Ciencias Sociales y Jurídicas de la Universidad Complutense de Madrid. No. 31, 2011, p.11. [en línea] <http://www.redalyc.org/redalyc/pdf/181/18120621004.pdf> [Consulta: 14/09/2012]

[17] "Ellsberg recordaría años más tarde como el capitán del navío estadounidense supuestamente atacado por patrulleras norvietnamitas envió un comunicado al Pentágono restándole importancia al supuesto suceso y recomendando que se olvidara ante la imposibilidad de confirmar que el hecho hubiera tenido lugar, justo lo contrario de lo que hizo la administración Johnson, que lo usó como excusa para lanzar el primer bombardeo contra Vietnam del Norte presentándolo como una represalia, e iniciando así la intervención militar directa de los Estados Unidos en Indochina(...)". SANCHEZ, op. cit., p. 12.

[18] SANCHEZ, op. cit., p. 12.

Iniciada ya la guerra, incluida la invasión terrestre norteamericana y habiendo realizado infinidad de informes, recibió el encargo de viajar a Vietnam para evaluar la situación. Ellsberg se convirtió durante casi dos años en casi un soldado más, y su visión acerca de la guerra poco a poco comenzó a cambiar, deteniéndose en errores militares y en errores históricos de la intervención de EE.UU. en el Sudeste Asiático desde sus inicios, terminando por convencerse de que el conflicto era completamente inviable. Luego, tras cuatro años de implicación personal sospechó que incluso los dirigentes de la guerra sabían ya en 1967 que no había posibilidades racionales de ganarla. Ellsberg fue dándose cuenta que su prolongación inútil era solamente por motivos políticos y para evitar asumir una derrota.[19]

I.2.1.1.a. El Informe. Los documentos a los que el "Informe McNamara", también denominados los *Pentagon Papers*, hacen referencia, son redacciones en las que Ellsberg colaboró en su primera etapa en el Departamento de Defensa, pero analizados.

En 1967 el a esas alturas ya titubeante Secretario de Defensa Robert S. McNamara, solicitó el estudio que a modo de resumen e investigación histórica evaluaría y determinaría las causas del fracaso, ya evidente a fines de ese año. El nombre original de la investigación era "*United States – Vietnam Relations, 1945 – 1967: a Study Prepared by the Department of Defense*". El encargo recayó en la *Rand Corporation*[20], institución a la que después de volver de Vietnam regresó Ellsberg como experto, al abandonar el Pentágono preso de la decepción. [21]

[19] Idem, p. 13.

[20] En su página institucional declara ser una institución sin fines de lucro que ayuda a mejorar la política y la toma de decisiones a través de la investigación y el análisis, enfocando su interés en cuestiones como la salud, la educación, la seguridad nacional, las relaciones internacionales, el derecho y el comercio, el medio ambiente, entre otros. Dice contar con un equipo de investigación formado por algunas de las mentes más prominentes del mundo y finalmente que como organización no partidista, son ampliamente

En el informe se examinaron los aspectos más confidenciales de las relaciones entre ambos países, incluyendo documentos de alto secreto referentes a tomas de decisiones erróneas, actuaciones inmorales, tergiversaciones y mentiras de cinco administraciones estadounidenses, desde Truman hasta Johnson.[22]

I.2.1.1.b. La filtración. Luego de leer las más de siete mil páginas de documentos tomó conciencia de la confirmación de sus sospechas iniciales y de las mentiras de sucesivos gobiernos respecto a Vietnam, decidiendo que la recopilación debería ser hecha pública y difundida.[23]

La parte más escabrosa revela que la administración Johnson sabía desde 1966 que la guerra no podría ser ganada nunca en los términos propuestos por los planificadores de la guerra (ir a Vietnam, acabar para siempre con los comunistas y retirarse.) Ni siquiera había razonables posibilidades de estabilizar y defender Vietnam del Sur.[24]

---

respetados por su funcionamiento independiente. [en línea] <http://www.rand.org/about/history.html> [Consulta: 14/09/2012]

[21] Idem.

[22] De hecho Truman (1945 - 1953), el primero en fijar su atención en Indochina, financió a los franceses para recuperar su excolonia en momentos en que ya se instalaba la legitimidad de los movimientos emancipadores anticolonialistas; Eisenhower (1953 - 1961) que al mismo tiempo promocionó la democracia y apoyó la dictadura de Vietnam del Sur, menoscabando las elecciones que unificarían a Vietnam según los acuerdos de Ginebra de 1954 "conciente de que estas serían ganadas por los comunistas en forma democrática"(p.18) ; Kennedy (1953 - 1963) amplió de mil a dieciséis mil la dotación en Vietnam mintiendo acerca de que con esa cantidad bastaba mientras sus propios asesores hablaban de que sería una causa perdida sin el envío masivo de mayores dotaciones; Johnson (1965 – 1969) lo ya dicho acerca del incidente de Tonkín, mintiendo para conseguir una guerra para obtener beneficios electorales; y Nixon (1969 - 1974) que prometió en 1968 terminar la guerra y reducir la presencia en 1969, la prolongó por cuatro años más con gigantescos bombardeos. SANCHEZ, op. cit., p. 14.

[23] SANCHEZ, op. cit., p. 15.

[24] Idem.

En 1969 comenzó secretamente a fotocopiar el informe junto a Anthony Russo, decidiendo en 1970 hacerlo público y concretándolo el 13 de Junio de 1971 con la ayuda del periodista Neil Sheehan, corresponsal del *The New York Time*s, un viejo amigo conocido en su etapa en Vietnam.[25]

I.2.1.1.c. La respuesta del gobierno. En un comienzo el gobierno no le dio importancia porque involucraba a administraciones anteriores, pero pronto cambiaron bruscamente de opinión consiguiendo incluso una orden judicial para prohibir la publicación. Pero la prensa estadounidense hizo causa común con el *The New York Times* y continuaron con la publicación de casi la totalidad de los papeles, así, si el gobierno quería evitar la publicación, tendría que comenzar un juicio contra cada director de periódico involucrado, comenzando procesos largos y tormentosos. Finalmente, en el histórico fallo del 30 de Junio de 1971 se declaró legal la publicación en atención a la libertad de expresión y de prensa.[26]

Ellsberg y Rosso de todas maneras fueron acusados de robo, conspiración y espionaje invocando la *Espionage Act*, además de recepción, retención y comunicación de documentos de la defensa nacional, llegando a arriesgar 115 años de cárcel.[27] El juicio fue finalmente anulado y sobreseído en 1973 al constatarse que el gobierno en su objetivo de una pena ejemplificadora mintió, estafó, ocultó pruebas, allanó ilegalmente e incluso intentó comprar al juez.[28]

[25] SANCHEZ, op. cit., p. 16.
[26] Idem.
[27] SANCHEZ, op. cit., p. 17.
[28] Idem, p. 18.

I.2.1.1.d. El escándalo Watergate. La anulación del juicio fue una de las consecuencias del Escándalo Watergate. La fuga llevada a cabo por el ex hombre del Pentágono y la imposibilidad de censurarla motivó al gobierno a formar la unidad de "Los fontaneros", cuyo objetivo fue ensuciarle la imagen pública a Ellsberg, evolucionando después hacia objetivos más políticos de cara a las elecciones de 1972, valiéndose de métodos al margen de la ley por el transcurso de casi un año. Tras dos años de escándalo, Nixon dimite en Agosto de 1974. [29]

I.2.1.2. El precedente tecnológico: Cryptome.org. Es un sitio *web* fundado en 1996 por John Young, un arquitecto de Nueva York. Su misión es la de publicar materiales que los gobiernos y las corporaciones preferirían mantener ocultos. Fue atacada por *Microsoft* y tuvo enfrentamientos con *Pay Pal*.[30]

En particular reciben material atingente a la libertad de expresión, la seguridad nacional, la privacidad, criptografía, tecnologías, inteligencia y secretos de gobierno. [31]

Cryptome aloja documentos que constan en más de 70.000 archivos, incluye fotografías de soldados estadounidenses muertos en Irak, listas de personas que se cree que son agentes del *MI6*, mapas detallados de las instalaciones del gobierno, la lista de los trabajadores de la *Stasi* en el momento de su disolución el 8 de diciembre de 1989, y 4.000 fotos de muertos y heridos en la guerra de Irak.[32]

---

[29] Idem.
[30] O´HAGAN, Andrew. "*Julian Assange. The Unauthorised Autobiography*". [*Julian Assange. La autobiografía no autorizada*]. Cannongate books, traducción de Enrique Murillo para Los libros del Lince/Catalonia bajo el título *"Julián Assange. La verdad amordazada. Autobiografía no autorizada."*, Santiago de Chile, 2012, p.140.
[31] [en línea] <http://en.wikipedia.org/wiki/Cryptome> [Consulta: 1/10/2012]
[32] *Idem.*

Es un sitio que se encuentra en la batalla a favor de la información en la Internet, pero Assange lo crítica de no tener la tecnología para proteger a las personas que le puedan proporcionar material, siendo un requisito imprescindible.[33]

I.2.1.2.a. La filtración en Agosto de 2000 de un informe de la CIA de 1998. El informe buscaba detallar a grandes rasgos la estructura de una delegación japonesa. Analizó por ejemplo sus recortes de personal (20.000 empleados menos en siete años), algunos detalles acerca de su presupuesto y sus principales objetivos de infiltración (Irán, China, Corea del Norte, Cuba y Rusia). La fuente era un ex agente japonés, Hinorari Noda, que buscaba saldar cuentas con sus antiguos jefes.[34]

Obviamente la filtración produjo preocupación en la inteligencia norteamericana, el FBI llamó a Young después de que la prensa se hiciera eco de la fuga, comunicándole las protestas del gobierno nipón y pidiéndole que retirara los nombres, lo que no hizo.[35]

I.2.1.2.b. La filtración de la "guía espía" de Microsoft[36]*. El documento filtrado* describe cómo *Microsoft* guarda datos privados de los usuarios de *MSN Messenger*, *Windows Live* y *Xbox Live*, y cómo esos datos se ponen a disposición de las autoridades de EE.UU. cuando son requeridos.

Luego de que en un principio *Microsoft* consiguió una medida judicial preventiva de bajar de la Internet el sitio, gracias a la movilización y presión de

[33] O´HAGAN, op.cit., p.140.
[34] EL PAÍS. *"John Young, Un indiscreto en la web"*, 13 de Agosto de 2000. [en línea] <http://elpais.com/diario/2000/08/13/sociedad/966117603_850215.html> [Consulta: 1/10/2012]
[35] *Idem.*
[36] THE GUARDIAN. *"Microsoft backs down over online spy guide"*. [Microsoft retrocede sobre la guía de espionaje en línea]. 25 de Febrero de 2010. [en línea] <http://www.guardian.co.uk/technology/blog/2010/feb/25/microsoft-cryptome-surveillance> [Consulta: 1/10/2012]

organizaciones de derechos civiles, retira su demanda y el sitio vuelve a estar *online*.

I.2.2. ¿Cuáles son los elementos esenciales de un Leaking?

I.2.2.1. La información y el productor de la información. En un principio, alguien produce la información. Luego de ello, el individuo o la institución tienen la opción de designar a la información como clasificada o no. En este último caso, la información es pública.[37] Sólo puede haber fuga cuando la información no es pública. ¿Quién o quienes son los generadores de la información en los *Pentagon Papers*? Los productores de la información en este *leak* son principalmente los investigadores y expertos de *Rand Corporation*, el Secretario de Defensa Robert S. McNamara, los ex Presidentes de EE.UU. Truman, Eisenhower, Kennedy y Johnson y todos los funcionarios y asesores de aquellas administraciones que hayan aparecido en los papeles realizando declaraciones o actuaciones que pongan en evidencia los actos reprochados. Claramente la intención de estos generadores de información era mantenerla reservada.

I.2.2.2. La fuente. Es la persona que teniendo la información realiza la fuga del material clasificado. Hay dos tipos de fuente:

a.- Interna. La fuente es un individuo que está vinculado de alguna manera con los generadores de la información o a la red informática y está autorizado para acceder al material, como Daniel Ellsberg; ó

b.- Externa. La persona no está vinculada a los productores de la información o está fuera de la red informática y no está autorizada a tener

[37] MAURER, Tim, *"WikiLeaks 2010: A Glimpse of the Future?"*. [Wikileaks 2010: Una ojeada al futuro]. Discussion Paper 2011-10, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, August 2011, p.7. [en línea] <http://belfercenter.ksg.harvard.edu/files/maurer-dp-2011-10-wikileaks-final.pdf> [Consulta: 21/09/2012]

acceso al material, pero accede o logra acceder a él desde el exterior,[38] en este último caso por ejemplo, a través del *kacking* o piratería, como la de los "hackers chinos" que se han infiltrado en las redes de numerosos gobiernos extranjeros[39].

I.2.2.3. La publicación. La fuente necesita de una infraestructura para lograr que el material se conozca ampliamente. Ellsberg, fuente en los *Pentagon Papers*, requirió de la ayuda de su amigo Neil Sheehan, periodista del *The New York Time*s para difundir su denuncia. De esta manera en aquel caso el *The New York Times* fue la publicación, dándole la posibilidad de que las copias del informe fueran distribuidas por toda su red nacional de ventas. En este caso, la distinción entre la fuente y la publicación fue fácil. La fuente tenía la información y la publicación contaba con la red de distribución para que la información sea conocida.[40]

La Internet obvía la necesidad de una red de distribución como la que necesitó Ellsberg en 1971. Cualquiera puede crear un sitio *web* con casi ningún costo, accesible a todos los usuarios de la *World Wide Web*. Así, en la era de Internet, una fuente puede también ser la publicación y la distinción se vuelve borrosa.

[38] MAURER, op. cit., p.7.
[39] EL PAÍS. *"Hackers chinos atacan la red militar de occidente"*. [en línea] <http://elpais.com/diario/2007/09/16/internacional/1189893604_850215.html> [Consulta: 21/09/2012]
[40] MAURER, op. cit., p.9.

I.2.2.4. La audiencia. Finalmente, las filtraciones tienen como objetivo el ser conocidas por una audiencia lo más amplia posible. En el pasado, el rango de exposición de una publicación se veía limitada por la infraestructura física y de publicación de la red de distribución. Internet expandió este rango de regional a global, salvo, que un gobierno tome medidas para limitar el acceso y censurar material como el de la República Popular de China.[41]

I.2.3. ¿Cuál es nuestro concepto de Leaking?

I.2.3.1. Concepto de Oxforddictionaries.com/. Lo reflexiona tanto como verbo, tanto como sustantivo.

Como verbo, por vía ejemplificatoria y a propósito de información secreta, le da un tratamiento doble, es decir, como "con objeto de" y como "adjetivo". "Con objeto de" revelar información secreta: El informe fue filtrado a la prensa. Como el "adjetivo" filtrado: El documento filtrado del gobierno.

Como sustantivo, sería una divulgación intencional de información secreta, ejemplificando con la frase: uno de los empleados fue el responsable de la filtración.

I.2.3.2. Concepto de Collinsdictionary.com/. También lo analiza desde ambas perspectivas siguiendo básicamente las mismas líneas anteriores.

I.2.3.3. Nuestro Concepto de Leaking. Habiendo recogido tanto el relato histórico, como el precedente tecnológico de *WikiLeaks*, los elementos esenciales aportados por investigadores y las acepciones utilizadas por diccionarios en idioma inglés podemos construir nuestro propio concepto de *leaking*. Y este es tomando la palabra en tanto verbo: "Acto de divulgación de

[41] *Idem,* p.11.

información clasificada como secreta para que sea conocida y reflexionada por una audiencia lo más amplia posible."

De esta manera y agregando nuestro concepto de *wiki*, podríamos conceptualizar a *WikiLeaks* desde un punto de vista literal, es decir, desde la denominación que le escogió su fundador como "un sitio *web* que otorga a toda la comunidad de usuarios de la Internet herramientas tecnológicas de rápido aprendizaje y fácil ejecución para constituir bases de datos de información secreta y que mediante su divulgación, se genere información y conocimiento disponible para todos, con el objetivo de que sea procesada por una audiencia lo más amplia posible y se facilite la transformación social."

I.3. ¿CÓMO SE ORIGINA y ESTRUCTURA WIKILEAKS?

I.3.1. Su contexto. La web 2.0.

I.3.1.1. ¿Qué es la web 1.0? En 1989, Tim Berners-Lee comenzó a trabajar en el CERN, *European Organization for Nuclear Research*. En él desarrolló el sistema que él y Robert Cailliau llamarían la *World Wide Web*. El objetivo del proyecto era proporcionar un entorno distribuido de hipertexto para permitir a los físicos compartir y distribuir fácilmente información.[42]

[42] HALL, Wendy. "*The Ever Evolving Web: The Power of Networks"*. [La Web en constante evolución: El poder de las redes]. International Journal of Communication 5, 2011, p. 655. [en línea] <http://eprints.soton.ac.uk/272374/1/evolvingwebfinal.pdf> [Consulta: 11/02/2013]

Los protocolos abiertos en los que se basa el modelo cliente-servidor de la Web - Protocolo de transferencia de hipertexto (HTTP) y el Lenguaje de marcado de hipertexto (HTML) - fueron los pilares de su éxito.[43]

El visor *web* original trabajado en el CERN podría ser utilizado desde cualquier ordenador del mundo. Sin embargo, fue el desarrollo del navegador *Mosaic* de NCSA (Centro Nacional para Aplicaciones de Supercomputación de la Universidad de Illinois en Urbana-Champaign) que realmente hizo la *web* tan universalmente popular. De repente la Web, a través de Moisés (y navegadores posteriores, como *Netscape* y, más tarde, *Microsoft Internet Explorer*), se convirtió en el interfaz de uso fácil de Internet.[44]

Lo que caracteriza a esta *web* 1.0 es que, en estos primeros años de la *web* los navegadores sólo permitían a los usuarios leer los documentos y sólo podrían escribir si eran capaces de producir HTML[45]. De esta manera podemos llamar a la *web* 1.0 la de los enlaces a documentos[46], lo que produce como natural consecuencia en el ámbito de la información, que el control de ella esté en manos de los medios de comunicación tradicionales presentes en Internet con sus portales de noticias.

I.3.1.2. ¿Qué es la web 2.0? A medida que la tecnología de navegación se ha ido desarrollando, los usuarios han podido interactuar más fácilmente en la *web*. Además, cada vez más individuos han podido acceder a la Internet desde casa o desde dispositivos móviles. Hoy, personas sin grandes conocimientos técnicos pueden escribir en la *web*[47]. Si en la web 1.0 los procesos comunicativos se dirigían desde un emisor a un otro o a muchos, en la 2.0 todo se abre para que sean directamente los usuarios quienes desarrollen

[43] HALL, op. cit. p. 656.
[44] *Idem.*
[45] HALL, op. cit. p. 657.
[46] *Idem*, p. 658.
[47] *Idem.*

sus propios procesos comunicativos. En lugar de ser impulsada por una institución, empresa o persona, surge una *web* en la que los participantes se sitúan al mismo nivel. [48]

Desde estas nuevas posibilidades de redacción y comunicación en el ciberespacio, han surgido nuevos medios de comunicación que están siendo impulsados cada vez menos por editores y tanto más por usuarios denominados Contenidos Generados por el Usuario (CGU). Se refiere a los medios de comunicación que se crean o producen por el público en general y no mediante profesionales remunerados y que se distribuyen principalmente a través de las tecnologías en línea de la *web* 2.0.[49]

Hemos visto la aparición de *blogs* y de *wikis*, y de aplicaciones como *Flickr* y *YouTube*, que nos permiten compartir información rápida y fácilmente. La aparición de las redes sociales, como *MySpace* y *Facebook*, nos permiten interactuar y comunicarnos de una manera que hasta hace poco sería materia de la ciencia ficción. Más recientemente, la aplicación *Twitter* de *micro-blogging*, nos ha sorprendido por las formas creativas en que las personas lo utilizan para comunicarse. [50] De pronto, la *web* ya no se trataba de una simple consulta, se trataba de conectar a las personas.[51]

---

[48] CEBRIÁN, Mariano. *"La Web 2.0 como red social de comunicación e información"*, Estudios sobre el Mensaje Periodístico, 2008, 14, p. 345-361, [en línea] <http://www.ucm.es/info/emp/Numer_14/Sum/4-04.pdf> [Consulta: 11/02/2013]

[49] DAUGHERTY, Terry, Eastin, Matthew S., Bright, Laura F. y Chu, Shu-Chuan. Chapter 7 Expectancy-Value: *"Identifying Relationships Associated with Consuming User-Generated Content"*. [Identificando relaciones asociadas con el consumo de contenido generado por el usuario]. En: EASTIN, Matthew S., DAUGHERTY, Terry y Burns, Neil M., *"Handbook of Research on Digital Media and Advertising: User Generated Content Consumption"*. [Manual de Investigación de Medios y Publicidad Digital: Consumo de contenido generado por el usuario]. Information Science Reference, 2011, p. 147.

[50] HALL, op. cit. p. 658.

[51] *Idem.*

Expertos académicos reconocen que los modelos tradicionales de los medios de comunicación ya no representan adecuadamente a los medios digitales, para lo cual la convergencia[52] puede servir como una representación cada vez más precisa. Como resultado, esta convergencia de los medios de comunicación a través de la tecnología continúa cambiando hacia un modelo de control de los medios centrado en las audiencias y lejos del modelo anterior que ha sido caracterizado como "editor-céntrica". [53]

I.3.2. ¿Quién crea WikiLeaks y quiénes son sus principales colaboradores?

I.3.2.1. Julian Assange. Es el fundador de *WikiLeaks.* Nació en 1971 en *Townsville*, Estado de *Queensland*, Australia[54].

[52] DAUGHERTY, op. cit., p. 148, citando a su vez a PERRY, David K. que establece en su libro *"Theory and Research in Mass Communication Contexts and Consequences"*. [La Teoría y la Investigación en Contextos de Comunicación de Masas y Consecuencias] Lawrence Erlbaum Associates, Inc., Publishers, 2002, ps. 66 y 67, que "un modelo de convergencia (Kinca & id Schramm, 1975; EM Rogers Y Kincaid, 1981) puede ser cada vez más adecuado. En el modelo, dos participantes, A y B, comparten información en un esfuerzo por llegar a un acuerdo. La comunicación es un proceso cíclico, con sólo un principio arbitrario, entre socios iguales. Según el modelo, la persona A expresa un mensaje, que B interpreta. B entonces expresa un mensaje y lo interpreta A. El intercambio continúa indefinidamente, y los participantes convergen en una comprensión mutua. La comprensión perfecta, sin embargo, no puede ocurrir. (…) Teniendo en cuenta todo esto, la nueva tecnología de los medios probablemente seguirá teniendo ciertas influencias democratizadoras. Por ejemplo, el público cada vez más tomará sus propias decisiones sobre el contenido, (…) en lugar de depender de porteros. Los modelos lineales a menudo han hecho que los investigadores minimicen o pasen por alto muchas preguntas de investigación potencialmente fructíferas. Los modelos de convergencia pueden ayudar a identificar tales preguntas, incluso en contextos de comunicación de masas tradicionales."

[53] *Idem.*

[54] O´HAGAN, op.cit., p.31.

Su madre, Christine, era hija de Warren Hawkins, descrito como un rígido y tradicionalista académico que se convirtió en director de estudios de un *college*. La familia, se instaló en Australia desde la Escocia del siglo XIX. A los 17 años abandona el hogar, vende sus cuadros, se compra una moto, una tienda de campaña, un mapa y viaja 2.500 kilómetros para llegar a Sydney e incorporarse a su paisaje contracultural.[55]

Su padre biológico es John Shipton. Ausente la mayor parte de su vida. Christine se enamoró de él a los 17 años, un joven rebelde que conoció en una manifestación contra la guerra de Vietnam en 1970. La relación terminó y él no juega un papel en la vida de Assange hasta que se reencuentran cuando tiene 25 años.[56] Hoy es uno de los promotores de la fundación de su partido político, el "Partido Australiano *WikiLeaks*" que según sus adherentes promoverá una mayor apertura del gobierno y la política, y combatirá la creciente intrusión en la privacidad.[57]

Su madre rehizo su vida sentimental con Brett Assange, actor y director de teatro. El apellido se cree proviene de *Ah Sang*, supuestamente un colono chino del siglo XIX. Su padre adoptivo ponía en escena y dirigía obras teatrales y su madre se encargaba del maquillaje, el vestuario, el diseño del escenario y además era titiritera. El estilo de vida nómada marca los primeros años de Assange. Cuando Julian tenía 7 u 8 años se divorcian. [58]

[55] LEIGH y Harding, op. cit., p. 49.
[56] *Idem*
[57] ABC, "Assange confirma que presentará su candidatura al Senado australiano en 2013". 14 de diciembre de 2012. [en línea] <http://www.abc.es/internacional/20121213/abci-assange-candidatura-senado-australiano-201212130235.html> [Consulta: 15/10/2012]
[58] LEIGH y Harding, op. cit., p. 50 - 52.

Luego su madre vuelve a emparejarse, ahora con un hombre mucho más joven que ella, Keith Hamilton, en una relación tormentosa. Según Assange, se trata de un sicópata, al parecer, miembro de una secta que recogía niños después de convencer a sus madres adolescentes de entregarlos. La madre de Assange intenta abandonar a Hamilton en 1982 según una transcripción judicial, lo cual provoca una batalla por la custodia de Jamie, medio hermano de Assange. Según documentos judiciales se trataba de un maltratador que se había mostrado "físicamente violento". Christine al verse perseguida por este hombre se vio obligada a huir repetidamente con sus hijos. Vivieron durante 5 o 6 años como fugitivos. Durante su niñez, Julián asistió a 37 colegios sin recibir calificaciones de ningún tipo. De adolescente, se radicó en Melbourne junto a su madre viviendo en al menos 4 refugios distintos.[59]

Cuando tenía 13 o 14 años su madre arrendó una casa frente a una tienda electrónica. Christine ahorró hasta regalarle su primer computador, un *Commodore 64*[60], que a los 16 años ya se había convertido en su conciencia[61]. Lejos de utilizarlo sólo para juegos se interesó rápidamente en entender su funcionamiento, proyectar su pensamiento en el ordenador y conseguir que este fuese capaz de hacer cosas nuevas. Pronto entendió que no era el único, que había más personas de su edad con los mismos intereses, de desentrañar el lenguaje de las computadoras. *Crackeando* códigos lograban que mejorase la codificación de los programas, y *picando* los códigos lograban que fuese más difícil descifrarlos, era una competencia entre los que codificaban y los que *crack*e*aban*, los primeros trabajaban a sueldo en empresas mientras que ellos estaban en un cuarto de sus casas.[62]

[59] LEIGH y Harding op. cit., p. 53.
[60] *Idem,* p. 54.
[61] O´HAGAN, op.cit., p.56.
[62] *Idem,* p.61-64.

Pero el verdadero amanecer de la revelación para Assange no vino con el ordenador sino que con el módem. Cuando tuvo uno, supo que todo había cambiado, que Australia y el mundo no volverían a ser lo mismo. A los pocos días de haber recibido su primer módem, desarrolló un *software* que permitía comunicar al mundo entero la manera de buscar otros módems.[63]

Lo que pretendía él y los primeros *hackers* era cruzar las barreras que alguien puso para impedir la entrada a un sitio, la mayoría de ellas, dice Assange, para defender intereses mercantiles, para conservar el flujo de los beneficios. Mientras que para los *hackers* se trataba de una batalla en la que luchaban dos talentos, con el tiempo dice que llegaron a descubrir que esas barreras eran siniestras, erigidas para limitar la libertad de la gente.[64] Era el comienzo de la ideología *hacker*.

Cada hacker tiene un alias, el suyo era *Mendax*, que tomó del *spendide mendax* de Horacio, que se podía traducir como "delicioso engaño".

Arpanet, Un sistema norteamericano con el que los australianos no podían al principio comunicarse, salvo que se formara parte del mundo universitario fue una de sus primeros *hackeos*, y así pudo colarse en él. También gustaba de adentrarse en los ordenadores del Octavo Grupo de Mando del Pentágono[65]. Su placer, dice, era el de conseguir entender el funcionamiento del sistema informático, llevarse ese conocimiento y hacer que fuese de dominio público[66].

[63] *Idem*, p.67.
[64] *Idem*, p.68.
[65] *Idem*, p.69-70.
[66] *Idem*, p.72.

En 1988, Assange *hackeó* Minerva, el sistema de la Comisión Australiana de Telecomunicaciones de Ultramar[67]. Ese mismo año, en el contexto de la pronta aprobación de una nueva ley de delitos informáticos, la policía trataba de encontrar ubicó a los *hackers* más aventajados de Australia en Melbourne. Se hicieron redadas y prontamente se llegó a buscar a Assange a su hogar, no hallándolo, pero comenzándose a vigilar sus llamadas telefónicas.[68] Assange borró todos sus discos, quemó los papeles que tenía impresos, se fue de la periferia de Melbourne y se radicó en el centro de la ciudad como *okupa*, con su novia. Tenía 18 años cuando la dejó embarazada de Daniel[69]. (Se casaron y luego de un tiempo se separaron. Assange debió pelear durante años para que dejaran visitarlo y así tener una relación con su hijo.[70])

En 1991 era el "hacker más completo de Australia" según *The Guardian.*[71] Junto a su grupo de amigos hackers: *Phoenix*, *Trax* y *Prime Suspect*, fundan la "Internacional Subversiva", desde la cual lanzaban expediciones nocturnas hacia el interior de la empresa canadiense de comunicaciones *Nortel*, y también al núcleo informático de la *NASA* y el Pentágono.[72] Además tenían una revista en la que ofrecían información acerca de cómo introducirse en los sistemas de telefonía ilegalmente y hacer llamadas gratuitas. La revista tuvo un público exclusivo: el mismo grupo de *hackers*.[73]

[67] MAURER, op. cit., p.14.
[68] O´HAGAN, op. cit., p.72 - 73.
[69] LEIGH & Harding, op. cit., p. 54.
[70] *Idem*, p. 60.
[71] THE GUARDIAN, *"Julian Assange: the teen hacker who became insurgent in information war"*. [Julian Assange: el hacker adolescente que se convirtió en una guerra informática insurgente]. 30 de enero de 2011. [en línea] <http://www.guardian.co.uk/media/2011/jan/30/julian-assange-wikileaks-profile> [Consulta: 2/07/2013]
[72] O´HAGAN, op. cit., p.72.
[73] THE GUARDIAN, *"Julian Assange: the teen hacker(…)"*, op. cit.

En la primavera de 1991, encontraron un blanco nuevo y emocionante: *MILNET*, la red de comunicación de las Fuerzas Armadas de los EE.UU. Rápidamente Assange descubrió una puerta trasera. "Hemos tenido el control total sobre ella durante dos años", afirmó más tarde. Los *hackers* también rutinariamente *hack*e*aban* los sistemas informáticos de la Universidad Nacional de Australia.[74]

Cuando finalmente el gobierno lo encontró, necesitó de tiempo para presentar acusaciones contra él en 1994[75]. En 1996[76] finalmente se inició el juicio en el que se incluían 31 imputaciones contra él, 26 contra *Prime Suspect* y 6 contra *Trax*[77]. Parte de esos delitos consistían en haber escrito artículos que publicaban en su propia revista grupal, además del daño que se le habría producido a la red informática de la Universidad Nacional australiana. Con el devenir del juicio, su compañero *Prime Suspect* se convirtió en testigo en su contra[78]. No hubo sentencia de prisión contra él, solo pagar una multa de 5.000 dólares australianos y pagar a modo de reparación a la universidad 2.100 dólares australianos. *Trax* salió también librado del juicio sin necesidad de pacto. Assange fue condenado a una multa de 50.000 y a la suma de 2.100 a modo de resarcimiento para la universidad.

[74] *Idem.*
[75] O´HAGAN, op. cit., p. 98.
[76] *Idem,* p. 99.
[77] *Phoenix* anteriormente ya había sido enjuiciado.
[78] O´HAGAN, op. cit., p. 105.

En unas palabras que hoy parecen proféticas, Galbally, su abogado defensor le dijo al juez: "es claramente una persona que quiere que Internet ofrezca a la gente material por el cual no se tenga que pagar, y el presta su servicio gratuito a esta causa".[79] El juez Leslie Ross dijo que aunque consideraba los delitos de Assange de suma gravedad, no existían pruebas que vincularan su actuar a un interés personal. Era, de hecho más "mirón" que malicioso y había actuado según palabras del juez, por "curiosidad intelectual"[80].

En 1997 colaboró como investigador para el libro de Suelette Dreyfus "*Underground: tales of hacking, madness & obsession on the electronic frontier*."[81] Trata en lo esencial acerca de la adolescencia del propio Assange y sus inicios junto al grupo de hackers de su misma edad, sus continuos cambios de escuela y casa, su intrusión en la red de los servicios de defensa estadounidenses y la persecución policial que vivió en su Australia natal.[82] Aparece como investigador pero su huella es palpable, hay partes que se leen como si fuera su biografía.[83]

Entre 2003 y 2006 estudió física y matemáticas, además de filosofía y neurociencia en la Universidad de Melbourne, la segunda en antigüedad del país, aunque no llegó a licenciarse. [84]

[79] LEIGH y Harding, op. cit., p. 60.
[80] *Idem*, p. 59.
[81] Hay traducción en español: *Underground. Historias de hackeo, locura y obsesión desde la frontera electrónica*, Seix Barral, Barcelona, 2010.
[82] En 2012 el libro ha sido la base de la película *Underground: The Julian Assange Story.*
[83] LEIGH y Harding, op. cit., p. 56.
[84] Idem, p. 61.

En 2006 escribió un nuevo ensayo que primero tituló “Estado y Conspiraciones Terroristas”, (fechada 10/11/2006) y que luego cambió por “Conspiración como Gobierno” (fechada 3/12/2006). En su introducción declara que “si hemos aprendido algo, es que los regímenes no quieren ser cambiados. Debemos pensar mas allá de los que nos han precedido y descubrir cambios tecnológicos que nos potencien con formas de actuar que nuestros antecesores no hubiesen podido (realizar).” [85]

Ese mismo año, funda *WikiLeaks.*

En Octubre de 2010 asegura que la estructura de la organización ya la conforman 12 personas fijas y que pronto serán 20. El número total de colaboradores ascendería a 800[86]. Aquí la versión de Assange es radicalmente opuesta a la de su ex colaborador más importante en la época de las filtraciones, Daniel Domscheit-Berg, para quien aun en los mejores tiempos apenas contaban con un puñado de personas a las que podían confiar las tareas de mayor relevancia y que en realidad eran Assange y él quienes llevaban la carga pesada. Agrega que nunca tuvo contacto con los disidentes chinos de los que hablaba el fundador del *Wiki*. Aun más, dice que cuando decían que tenían miles de voluntarios y cientos de ayudantes activos se trataba solo de una lista de correo de quienes alguna vez comunicaron su deseo de apoyar el proyecto, sin evolucionar desde el estado de una lista de nombres.[87]

Veamos cuales han sido los colaboradores más importantes.

[85] [en línea] < http://cryptome.org/0002/ja-conspiracies.pdf > [Consulta: 15/10/2012]
[86] EL PAÍS. “Cita secreta con el hombre que hace temblar al Pentágono”. 24 de Octubre de 2010. [en línea] <http://elpais.com/diario/2010/10/24/domingo/1287892353_850215.html> [Consulta: 26/09/2012]
[87] DOMSCHEIT-BERG, Daniel, *“Inside WikiLeaks”*. Traducido por Ana Duque de Vega y Carles Anfreu Saburit bajo el título *“Dentro de Wikileaks. Mi etapa en la web más peligrosa del mundo”*, Rocaeditorial, 2011, p. 30.

I.3.2.2. Daniel Domscheit-Berg. Su principal colaborador. Nació en 1978. Al momento de tomar conocimiento de la existencia de *WikiLeaks* en Septiembre de 2007, residía en *Wiesbaden* y tenía un trabajo fijo como diseñador de redes y responsable de su seguridad para *Electronic Data Systems*, una importante empresa estadounidense que se encargaba de las necesidades de tecnología informática de clientes civiles y militares, con su principal sucursal en *Rüsselsheim*, Alemania. Según un acuerdo tácito no se encargaba de los clientes militares, así, era responsable principalmente de *GM* y por vía de consecuencia de *Opel* y de varias compañías aéreas, ganando unos 50.000 euros al año.[88]

Luego de la filtración de los manuales de Guantánamo, se convenció en intentar participar del proyecto y se registró en el *chat* de la página *Wikileaks.org* preguntando si podía colaborar de algún modo. La respuesta llegó dos días más tarde, Assange le asignó un par de tareas poco importantes. Enseguida se le ocurrió la idea de incluir a *WikiLeaks* en el programa del XXIV *Chaos Communication Congress*, la cita anual de *hackers* y otros protagonistas del mundo de la informática que tiene lugar entre Navidad y Año Nuevo en el Centro de Congresos de Berlín, organizado por el *Chaos Computer Club*. Allí se conocieron[89].

[88] DOMSCHEIT-BERG, op. cit., p. 19.
[89] Idem, p. 18.

Comenzó a colaborar directamente en una publicación desde enero de 2008 con la filtración de los documentos del banco *Julius Bär*[90]. Con el tiempo su participación se hizo cada vez más importante y absorbente, hasta que decide dejar su trabajo a tiempo completo en enero de 2009. Fue ganando la confianza de Julian Assange hasta convertirse en determinante para el proyecto, ocupando el cargo de segundo vocero de *WikiLeaks* con el seudónimo de *Daniel Schmitt*[91].

Participa en la mayoría de las filtraciones de *WikiLeaks* alcanzando hacia el final de su ingerencia a colaborar en los diarios de guerra de Afganistán. Pero por profundas desavenencias y disputas con Assange, desde la utilización de la cuenta *Twitter* de la organización para fines personales de Assange, hasta la administración del dinero de las donaciones, se retira el 15 de septiembre de 2010, junto a Birgitta Jonsdottir, miembro del Parlamento de Islandia que había apoyado a *WikiLeaks* desde el verano de 2009, así como con una docena de otros miembros de izquierda de *WikiLeaks*.[92]

I.3.2.3. Kristinn Hrafnson, el actual portavoz. Periodista islandés que trabajó durante 20 años en la televisión estatal: "Tenía ganas de trabajar en historias que crean grandes olas en el mundo", explicó.[93]

I.3.2.4. Birgitta Jónsdóttir. Parlamentaria islandesa. Miembro del *Movement*, un partido nuevo que accedió al Parlamento debido a la crisis económica y los movimientos sociales. Activista del movimiento de derechos civiles, fanática del Tíbet que había viajado por todo el mundo y escritora de poesía. [94]

[90] *Idem*, p. 26.
[91] *Idem*, p. 28.
[92] MAURER, op. cit., p.10.
[93] EL PAÍS. *"Cita secreta…"*, op. cit.
[94] DOMSCHEIT-BERG, op. cit., p. 110.

En conjunto a Assange y Domscheit-Berg además de otros colaboradores y activistas buscaron convertir en ley la *IMMI* (*Icelandic Modern Media Iniciative*) [95] El proyecto busca hacer de Islandia un país en el que se garantice la libertad de información, protegiendo a quienes revelen información de interés público y a las fuentes anónimas, dándole protección también a las comunicaciones periodista-fuente, a los intermediarios, etc.[96]

I.3.2.5. Otros colaboradores.

Sarah Harrison y Joseph Farrell. Ayudantes personales, periodistas en práctica que administraban su correo electrónico y su agenda.

James Ball. Experto en datos de *WikiLeaks*.

Vaughan Smith. Antiguo capitán del *Grenadier Guards*, fundador del *Frontline Club* y anfitrión de Assange en *Ellingham Hall*.

Jacob Appelbaum. Representante de *WikiLeaks* en EE.UU. *Hacker* voluntario de *WikiLeaks*, residente en Seattle.[97]

Daniel Ellsberg. Filtró los papeles del pentágono en 1971. Aceptó la propuesta de Assange de implicarse en *WikiLeaks* y ha permanecido fiel desde un primer momento hasta ahora. [98]

El informático y el arquitecto. Ambos expertos en informática, claves para la continua mejora en la estructura informática de la página *web* y el diseño de su seguridad.[99]

---

[95] *Idem*, p. 124.
[96] [en línea] <http://en.wikipedia.org/wiki/International_Modern_Media_Institute> [Consulta: 3/11/2012]
[97] LEIGH y Harding, op. cit., p. 67.
[98] *Idem*.
[99] DOMSCHEIT-BERG, op. cit., p. 113.

Mikael Viborg. Dueño del servicio de Internet sueco *PRQ*, proveedor de *WikiLeaks*.

Ben Laurie. Matemático británico experto en codificación. Se dedica a arrendar búnkers "a prueba de bombas" para albergar servidores comerciales de la Internet.[100] Assange le propuso como proyecto una "agencia de inteligencia democrática de código abierto"[101].

Mwalimu Mati. Jefe del *Mars Group Kenya*, una organización anticorrupción. Fue quién entregó a *WikiLeaks* el informe reservado acerca de la corrupción del ex presidente Daniel Arap Moi.[102]

Smari McCarthy. Programadora y defensora de la *Modern Media Iniciative*. Residente en Islandia.

Rop Gronggrijp. Hacker holandés, hombre de negocios, amigo de Assange y defensor de la *Modern Media Iniciative.*

Herbert Snorrason. Defensor de la *MMI*.

Donald Böstrom. Periodista sueco y contacto de *WikiLeaks* en Estocolmo.

Daniel Mathews. Compañero de Julian Assange en la facultad de ciencias exactas, fue quien más lo ayudó a preparar todos los documentos relativos a la fundación de *WikiLeaks* y más adelante, quien escribió un análisis sobre el primer documento filtrado en la web.[103]

Israel Shamir. Famoso negador del holocausto y antisemita. Según Domscheit-Berg, uno de los motivos por los que deja *WikiLeaks*.

[100] LEIGH y Harding, op. cit., p. 68.
[101] *Idem*.
[102] *Idem*, p. 74.
[103] O´HAGAN, op. cit., p.141.

Johannes Wahlström. Periodista sueco, hijo de Israel Shamir. Contrario a tener los mismos cuidados de edición con cables que no tendrían un gran impacto en los medios, los cuales cifraban varios miles, aun por solicitud de ONGs y activistas de Derechos Humanos que solicitaban la protección de la identidad de víctimas de crímenes espantosos.[104]

Anonymous. La organización les colaboró determinantemente con la filtración de la Cienciología.y ordenaron el *wiki* para que los lectores pudieran manejar el caudal de esos documentos.[105]

I.3.3. ¿Cuál era la base tecnológica de WikiLeaks?

I.3.3.1. Los portátiles y la comunicación interna. Los portátiles de *WikiLeaks* tenían codificación de grado militar. Si caían en manos ajenas sus datos no podían ser descifrados, ni siquiera directamente desde el disco.[106] El servicio por telefonía de Internet *Skype*, que también hace uso de la codificación, era muy popular en el grupo para mantener conversaciones cotidianas caseras. Como fue desarrollado en Suecia, no en Estados Unidos, el equipo confió en que no tenía una puerta trasera por la que la Agencia de Seguridad Nacional estadounidense pudiera meterse en las discusiones. [107] Para el año 2010, *WikiLeaks* tenía teléfonos encriptados y localizadores satelitales. [108]

---

[104] EL PAÍS. "*Por qué abandoné Wikileaks"*. 4 de Septiembre de 2011. [en línea] <http://elpais.com/diario/2011/09/04/internacional/1315087207_850215.html> [Consulta: 26/09/2012]
[105] DOMSCHEIT-BERG, op. cit., p. 46.
[106] "No podíamos mandar los correos desde nuestros portátiles, sino que debíamos hacerlo a través de máquinas remotas, por lo que las conexiones eran lentísimas.(…)" DOMSCHEIT-BERG, op. cit., p.62
[107] LEIGH y Harding, op. cit., p. 68.
[108] DOMSCHEIT-BERG, op. cit., p. 121

I.3.3.2. Los servidores. La infraestructura técnica de *WikiLeaks* consistió, durante la mayor parte de sus tempranos días, de solo un servidor, aunque tenían claro que hacia el exterior debían disimular haciendo parecer su infraestructura algo mucho más complejo.[109] Desde 2008, el servidor principal se situó en Suecia, que tiene leyes muy estrictas de protección a la libertad de expresión. A mediados de 2010, *WikiLeaks* utilizó alrededor de 50 "servidores ubicados en países con las leyes más favorables y la mejor protección de fuentes"[110].

I.3.3.3 El proveedor. La empresa de alojamiento web llamada *PRQ* ubicada en Estocolmo proporcionaba a *WikiLeaks* una cara externa. El propietario de *PRQ* declaro en una entrevista de la televisión sueca: "Al principio querían pasar a través de nosotros para saltarse las prohibiciones en lugares en los que *WikiLeaks* no era bienvenido, pero más tarde instalaron un servidor aquí". "Ofrecemos servicios de anonimato, túneles *VPN* (*Virtual Private Network*). El cliente se conecta a nuestro servidor y descarga información. Si alguien en la fuente de información intenta seguir su rastro, sólo llegará hasta nosotros, y nosotros no le revelaremos quien era el usuario de número de *IP* (protocolo de la Internet). Aceptamos cualquier cosa dentro del marco legal sueco, sin tener en cuenta lo censurable que sea. Nosotros no hacemos juicios morales." Esta actitud inflexible atrajo a Domscheit-Berg. [111]

[109] Idem, p. 31.
[110] *Idem*, p. 125.
[111] LEIGH y Harding, op. cit., p. 67.

I.3.3.4. Los sistemas de encriptación. Assange y su equipo han dicho que utilizan *OpenSSL* (un sistema de conexión segura de código abierto, como el utilizado por proveedores virtuales como *Amazon*), *FreeNet* (un método para compartir archivos *peer-to-peer* entre cientos o miles de ordenadores sin revelar su origen ni su propietario) y *PGP* (el sistema criptográfico de código abierto, abreviado de su jocoso nombre "*Pretty Good Privacy*"). [112]

[112] *Idem*, p. 68.

Pero el principal dispositivo de protección de anonimato que utilizaron fue *Tor*, una herramienta importante en los trabajos de espionaje de las agencias de inteligencia estadounidense. Fue un proyecto desarrollado en 1995 por la *US Naval Research Laboratory* y ha sido adoptado por *hackers* de todo el mundo. Utiliza una red de unos 2.000 servidores informáticos globales y voluntarios a través de los cuales puede circular cualquier mensaje, de manera anónima e imposible de rastrear, a través de otros ordenadores *Tor* y finalmente hasta un receptor fuera de la red. Lo clave es que no se pueda nunca vincular el emisor y el receptor analizando paquetes de datos. Pero *Tor* tiene un interesante punto débil: si un mensaje no está especialmente codificado desde el principio, su contenido real puede a veces ser leído por terceros. Esto tendría mucho que ver con el lanzamiento de *WikiLeaks* y la cantidad de documentación obtenida según los periodistas del *The Guardian*, quienes relatan hechos que podrían implicar a Assange. Dicen que antes de la primera publicación, escribe un mensaje a John Young de *Cryptome*: "Los *hackers* monitorean la inteligencia china y otras a medida que hurgan en sus objetivos, cuando tiran (*they pull*) y nosotros también. Una mina inagotable de material. Cerca de 100.000 documentos/e-mails diarios. Estamos a punto de abrir el mundo como un melón y dejar que florezca en forma de algo nuevo (…)".[113]

Domscheit-Berg en su libro explica cómo protegían a sus fuentes: "Nos encargábamos de que antes de llegar a nuestras manos, los documentos de informaciones explosivas dieran tantos rodeos, pasaran por tantos procesos de cifrado y de eliminación de identidad como fuese posible, para que nadie lograra seguirles la pista. Ni siquiera nosotros mismos podíamos contactar con nuestras fuentes, por mucho que se tratara de algún asunto urgente. Nuestros remitentes no dejaban rastro alguno en la red, ni la menor huella dactilar, ni un solo *byte* que pudiera delatarlos."[114]

[113] *Idem*, p. 69 - 71.
[114] DOMSCHEIT-BERG, op. cit., p.45.

I.3.4. ¿Cómo se financió?

Esencialmente a través de donativos. Desde 2008 contaban con 3 cuentas *PayPal.*[115]

En Abril de 2008 abrieron una cuenta en *Moneybookers* sobretodo para los donantes *online* de Estados Unidos. Nadie sabe cuanto se llegó a recaudar porque Julian Assange impidió el acceso. Luego abrió otra cuenta a su nombre a través de la misma empresa. [116]

Despues de la XXVI *Chaos Communication Congress* de diciembre de 2009 recibieron muchas transferencias a través de la Fundación Wau Holland, que gestionaba una cuenta corriente de *WikiLeaks* en Alemania. En el verano de 2010 ya tenían 600.000 dólares.

Un benefactor un tanto especial fue el mismo Adrian Lamo: un ex *hacker* más o menos famoso que más tarde seria el responsable de la detención de la supuesta fuente más relevante en las grandes filtraciones, el soldado Bradley Manning.[117]

I.3.5. ¿Cuáles fueron los primeros pasos de WikiLeaks y sus primeras filtraciones?

En 1999 Julian Assange fundó *leaks.org*, desde su perspectiva ya se había producido una convergencia entre activismo y tecnología. El sitio era tan incipiente que no tenía de qué nutrirse y no llegó a ninguna parte, pero de todas formas permaneció la idea de volver a intentarlo.[118]

Cuando algunos años después estuvo preparado para lanzarse a fundar *WikiLeaks*, la gran pregunta que se formuló fue ¿Cómo reducir el poder de las conspiraciones? La respuesta, dijo, “era algo que parecía estar a nuestro

[115] Tras el caso *Julius Bär*, el 1° de Marzo llegaron 1.900 euros, el 3 de marzo 3.700, el 11 ya se había acumulado 5.000. En Agosto llegaron a los 35.000 dólares.*Idem*, p.76.
[116] *Idem*, p.80.
[117] *Idem*, p.64.
[118] O´HAGAN, op. cit., p.115.

alcance: poniendo sus secretos al descubierto". "Nuestra tarea consiste en ponerle freno al poder que utiliza la conspiración de forma sistémica e impedir que actúe y que piense de manera eficiente. Y, a escala global, el modo de impedirlo consiste en poner al alcance de los ciudadanos la información que delata esa forma de proceder".[119]

WikiLeaks fue registrado el 4 de octubre de 2006[120], comenzando sus publicaciones el 28 de Diciembre[121].

La Declaración de propósitos de *WikiLeaks* expresó que "nuestro principal interés son los regímenes opresivos de Asia, el antiguo bloque soviético, el África subsahariana y Oriente Medio, pero también esperamos ser de ayuda a aquellos en Occidente que desean revelar comportamientos poco éticos en sus propios gobiernos y corporaciones." [122]

La presentación pública de *WikiLeaks* se realizó en el Foro Social Mundial de Nairobi, Kenya en 2007. Assange dio una exposición que sugirió una agenda política para lograr un gobierno abierto a través de la filtración masiva.

I.3.5.1. La primera publicación: La Unión de Cortes de Somalia.

I.3.5.1.a. La información y el productor de la información. La Unión de Tribunales estaba en contra del Gobierno de Transición e intentaba cambiar las cosas en el contexto de muchos años de violencia en Somalia, que había sufrido la secesión de más de sus dos terceras partes. La UT trató de ordenar el caos y la gente empezó a sentirse más segura en Mogadiscio estableciendo incluso sistemas de cuidado del aseo de la ciudad, un sistema de recogida de basuras por primera vez en once años.[123]

[119] *Idem*, p. 131 - 132.
[120] *Idem*, p.140.
[121] *Idem*, p.142.
[122] LEIGH y Harding, op. cit., p. 63.
[123] O´HAGAN, op. cit., p.142 - 143.

El documento filtrado parecía ser una carta firmada por un comandante militar, en la que utilizaba la fórmula raramente usada de "República Islámica de Somalia", escribiendo que el Gobierno de Transición se dedica a perseguir a los líderes religiosos somalíes y a los musulmanes en general, intentando convencer a la comunidad internacional de que los líderes son miembros de Al Qaeda. Los correos electrónicos interceptados sugerían además que algunos ministros somalíes en especial el del Petróleo, estaban dispuestos a reunirse con funcionarios chinos, adquiriendo importancia por ser de interés público la actitud del Gobierno hacia China y de China hacia África en general. Así, en un par de documentos se podía intuir la complejidad de la situación.

Estados Unidos se oponía a la UT a través de Etiopía, pues veían cualquier clase de politización islamista en África Oriental como algo relacionado con el ataque a la embajada en Nairobi en 1998. Así, justo después de que *WikiLeaks* había preparado las filtraciones, Etiopía ayudada por EE.UU. invadió Somalia.[124]-[125]

Según palabras de Assange, aunque el documento no fuera auténtico, planteaba cuestiones importantes y ayudaba a mejorar la comprensión de situaciones políticas complejas, pareciéndole ser un buen primer paso para *Wikileaks*.[126]

---

[124] *Idem*.

[125] "Tras perder el poder, las Cortes se partieron en dos bloques, los "moderados" encabezados por el jeque Sharif Ahmed, después presidente provisional de la mano de Washington, y los "radicales". De los segundos surge como fuerza dominante Al Shabab; dos años después reconquistó casi todo lo perdido." "Kenia opera desde hace meses dentro de Somalia de parte de EE.UU. Kenia reemplaza a Etiopía como fuerza extranjera". "La milicia islámica radical Al Shabab (Juventud) ha abandonado su último enclave importante en Somalia, pero aún no ha perdido la guerra. Tropas leales al Gobierno de Mogadiscio y soldados de la Unión Africana han entrado en Kismayo, al sur. No hubo combates ni muertos. Los islamistas se marcharon sin presentar batalla. Repiten la táctica de diciembre de 2006 en Mogadiscio: no presentar batalla ante una fuerza superior. ¿Cuál es su alternativa? ¿Bombas y atentados suicidas? Tratarán reagruparse y contraatacar." EL PAÍS. *"¿Quién diablos manda en Somalia?"*. 1 de Octubre de 2012. [en línea] <http://blogs.elpais.com/aguas-internacionales/2012/10/quien-diablos-manda-en-somalia.html> [Consulta: 10/10/2012]

[126] O´HAGAN, op. cit., p.142 - 143.

I.3.5.1.b. La fuente. Esta publicación estaba basada en un documento de misteriosa procedencia y hecha llegar a *WikiLeaks*, según Julian Assange, a través de fuentes chinas.

I.3.5.1.c. La publicación. WikiLeaks.org.[127]

I.3.5.1.d. La audiencia y las reacciones. La audiencia son todas las personas que se enteraron de la noticia a través de la página *web*. La página recién hacía su primera publicación y no tenía una relevancia como para llamar la atención de los medios. Además, los destinatarios directos de la información se veían invadidos por el ejército de Etiopía.

I.3.5.2. La revelación de la corrupción del ex líder keniano Daniel Arap Moi.

I.3.5.2.a. La información y el productor de la información. En agosto de 2007 comienza la búsqueda de una mayor repercusión en los medios. La filtración de un informe secreto de 110 páginas, destapa una red de empresas ficticias en 30 países para canalizar cientos de millones de euros desviados desde las arcas públicas.

La información fue explosiva entre otras cosas porque citaba los nombres de los bancos de Zurich y Londres como aquellos donde iba a parar el dinero y menciona con detalle propiedades e intereses económicos tanto en Estados Unidos como en Kenia. Además mostraba que el sistema financiero internacional estaba manchado con estas enormes sumas de dinero.[128]

I.3.5.2.b. La fuente. El informe, fue encargado por el gobierno de Kibaki a *Kroll Asociates* para chantajear Daniel Arap Moi, antiguo presidente de Kenia y

[127] WIKILEAKS. "Union of Islamic Courts". [en línea]
<http://www.wikileaks.org/wiki/Union_of_islamic_courts.zip> [Consulta: 10/10/2012]
[128] O´HAGAN, op. cit., p. 164.

aun factor en la política. Mwalimu Mati, Jefe del *Mars Group Kenya*, una organización anticorrupción, fue quién hizo llegar el documento.

I.3.5.2.c. El editor. La publicación fue realizada por el diario británico *The Guardian.*[129] *WikiLeaks* hizo las veces de intermediario/fuente.

I.3.5.2.d. La audiencia y reacciones. Los demás diarios británicos apenas se hicieron eco de la noticia. Pero en Kenia la reacción fue gigantesca en los medios, siguieron la línea de *The Guardian* pero con un poco más de cautela. Quedó en el ambiente la idea de que por más que Kibaki prometía luchar contra la corrupción la estaba encubriendo para sus propios propósitos de chantajear políticamente a Moi.

I.3.5.3. La publicación del manual del centro de detención de Guantánamo.

I.3.5.3.a. La información y el productor de la información. En noviembre de 2007 *WikiLeaks* filtra documentos oficiales acerca de los procedimientos que se llevan a cabo dentro de esta cárcel estadounidense.

Después del 11 de Septiembre de 2001 la administración Bush autorizó a que los presos interrogados en Guantánamo pudieran ser sometidos a torturas, tales como golpearles en la cabeza, simular intentos de asfixia, someterlos a bajas temperaturas o dejarlos en largos periodos de aislamiento con el único objetivo de sacar información sobre Bin Laden y sus colaboradores.[130]

Assange lo describe como "un documento increíblemente moderno, un texto que podemos imaginar que dentro de cien años será leído por todos los

[129] THE GUARDIAN. *"The looting of Kenya"*. [El saqueo de Kenia]. 31 de Agosto de 2007. [en línea] <http://www.guardian.co.uk/world/2007/aug/31/kenya.topstories3?INTCMP=SRCH> [Consulta: 10/10/2012]

[130] EL PAÍS. *"Guantánamo como telón de fondo"*, 3 de Mayo de 2011. [en línea] <http://internacional.elpais.com/internacional/2011/05/03/actualidad/1304373617_850215.html> [Consulta: 10/10/2012]

que deseen entender cabalmente la lucha ideológica (y mental) que se vivió en nuestro tiempo[131]".[132]

I.3.5.3.b. La Fuente. No se informa o no se conoce.

I.3.5.3.c. La publicación. WikiLeaks.org[133]

I.3.5.3.d. La audiencia y las reacciones. Durante una semana después de realizada la publicación, no pasó nada, pero intempestivamente llegó una carta del Comando Sur, responsable de Guantánamo, pidiendo que se retirase el documento de circulación, lo que según Assange demostraba su autenticidad. *WikiLeaks* no se hizo cargo de la solicitud. Luego la historia fue publicada por la revista *Wired*, y más tarde por el *The New York Times* y el *The Washington Post.*[134]

Edward M. Bush, portavoz de relaciones públicas de la cárcel de Guantánamo, respondió a la filtración diciendo que las cosas ya no se llevaban de esa manera. *WikiLeaks* filtró uno más actualizado y resultó en todo caso que las cosas iban de mal en peor. En la prisión ahora se suma la práctica de llevar a cabo juicios ficticios.[135]

I.3.5.4. La filtración sobre la sucursal del banco suizo Julius Bär en Islas Caimán.

---

[131] O´HAGAN, op. cit., p.142 - 143.
[132] La prisión fue creada por George W. Bush en 2002 al margen de las leyes nacionales e internacionales. Cerrar el penal fue la primera promesa de Barack Obama tras asumir el cargo en enero de 2009. El anuncio, en Marzo de 2011, de que se reanudarían los juicios en las comisiones militares fue el reconocimiento de su fracaso**.** EL PAÍS. *"Los abusos de Guantánamo"*, 25 de Abril de 2011. [en línea] <http://www.elpais.com/articulo/internacional/abusos/Guantanamo/descubierto/elpepuint/20110425elpepuint_4/Tes> [Consulta: 10/10/2012]
[133] WIKILEAKS, *"Camp Delta Standard Operating Procedure"*. [Procedimiento de Operación Estándar Camp Delta]. [en línea] <http://wikileaks.org/wiki/ Camp_Delta_ Standard_Operating_Procedure > [Consulta: 10/10/2012]
[134] O´HAGAN, op. cit., p.151.
[135] *Idem*, p.154.

I.3.5.4.a. La información y el productor de la información. El más grande de los bancos suizos fue acusado de malas prácticas en Enero de 2008 mediante una nueva filtración de *WikiLeaks*. Corresponde a la primera filtración en que participa Domscheit-Berg que detalla de la siguiente manera el modo de operar de la institución financiera: "Gracias a aquellos documentos podía comprenderse cómo se habían ocultado fortunas millonarias ante posibles inspecciones fiscales y se ponía de manifiesto mediante casos concretos. Se trataba de fortunas entre 5 y 100 millones de dólares por cliente (…). El refinamiento del banco era sorprendente. Un complejo sistema de compañías subsidiarias y transacciones financieras garantizaba que el dinero ubicado en Islas Caimán no solo estuviera protegido de intervenciones fiscales. El banco ocultaba los flujos de efectivo en interés de sus clientes, pero al hacerlo también se llenaba los bolsillos a espuertas. Me impresionó la inteligencia de las personas que habían ideado aquel sistema."[136]

I.3.5.4.b. La fuente. Rudolf Elmer. Había dirigido durante 8 años la sucursal de *Julius Bär Bank* en las Islas Caimán. Después de mudarse a Mauricio y de intentar vanamente atraer el interés de las autoridades por evasión de impuestos flagrante por parte de algunos clientes de su antigua entidad, se puso en contacto con Assange para publicar sus documentos.[137]

I.3.5.4.c. El editor. Wikileaks.org[138]*.*

I.3.5.4.d. La audiencia y las reacciones. Mediante la firma de abogados *Ludley & Sanger* se presentaron alegaciones ante un tribunal de San Francisco, California. Dijeron que "se trataba de "secretos empresariales" robados por un antiguo trabajador que de este modo había transgredido un acuerdo escrito de confidencialidad"[139]. Lo primero que hizo el juez fue revocar el dominio

[136] DOMSCHEIT-BERG, op. cit., p. 18.
[137] LEIGH y Harding, op. cit., p. 78.
[138] [en línea] < http://www.wikileaks.org/wiki/Bank_Julius_Baer > [Consulta: 15/11/2012]
[139] DOMSCHEIT-BERG, op. cit., p. 29.

WikiLeaks.org y exigió que se informara quién lo había registrado y desde qué dirección. *Dinadot*, el servidor, cedió de inmediato y cerró la página.

Pero la inscripción del dominio en San Francisco tenía precisamente la intención de que se encendiera un debate con la *American Civil Liberties Union*, el Comité de Defensa de la Libertad de Prensa y otras muchas organizaciones, además esta ciudad es el centro de gravedad de la cultura *ciberpunk*.[140]

Pronto *Bär* perdería completamente la guerra: *WikiLeaks* conservó el acceso a otras páginas albergadas en Bélgica y en otros países y aparecieron varias "páginas espejo" en las que había colgado el material denunciado[141], es decir, tan pronto como alguien eliminaba un sitio de la red, en otro lugar del mundo se creaban cientos de réplicas[142].

En lo estrictamente judicial, ganó por completo las alegaciones sucesivas y la página volvió a ser conectada, tuvo a su favor veintidós organizaciones y un batallón de abogados, el *The New York Times* publicaba crónicas poniéndose de su parte y la *CBS* al hacer público su número de dominio tituló el reportaje como "El número de la libertad de expresión". La sentencia fue interpretada como una victoria decisiva para todos los grupos en defensa de la Primera Enmienda de los Estados Unidos,[143]aunque claro, fue motivada por el desistimiento de *Julius Bär* al retirar la demanda por lo que doctrinariamente no contendrá sustancia para la discusión de fondo.

Pero en lo relacionado con los objetivos de *WikiLeaks*, los vientos soplaban a su favor. A principios de 2008 y en el transcurso de muy pocos días pasaron a ser conocidos, sin la demanda no hubieran podido conseguirlo tan rápido.[144]

[140] O´HAGAN, op. cit., p.173 - 174.
[141] LEIGH y Harding, op. cit., p. 78.
[142] DOMSCHEIT-BERG, op. cit., p. 29.
[143] O´HAGAN, op. cit., p.174.
[144] DOMSCHEIT-BERG, op. cit., p. 30.

I.3.5.5. La filtración sobre los grandes deudores del banco islandés Kaupthing.

I.3.5.5.a. La información y el productor de la información. El 1° de Agosto de 2009 se publicó el material que demostró que socios y allegados del Banco habían recibido créditos en condiciones especialmente ventajosas, justo antes de que el banco se declarara insolvente. Los deudores apenas ofrecerían garantías, en ocasiones ninguna, accediendo a créditos por muchos millones.[145]

I.3.5.5.b. Fuente. No informada y/o no conocida.

I.3.5.5.c. El editor. Wikileaks.org[146]

I.3.5.5.d. La audiencia y las reacciones. Los islandeses se lanzaron en masa a las calles para manifestarse. La indignación alcanzó a Inglaterra y los Países Bajos, residencia de muchos de los deudores. Los islandeses comprendieron la explotación de la que serían objeto: deberían pagar la quiebra de su Estado y de la seguridad social durante generaciones, mientras los banqueros se llenaban sus bolsillos.[147]

Poco después Assange y su grupo fueron invitados a Islandia para participar en una conferencia universitaria de libertades digitales, donde nació la idea de hacer de Islandia un puerto franco para los medios.[148]

I.3.5.6. Premio de la Prensa de Amnistía Internacional. En junio de 2009 *WikiLeaks* recibió este reconocimiento.[149]

---

[145] *Idem*, p. 103.
[146] WIKILEAKS, *"Financial collapse: Confidential exposure analysis of 205 companies each owing above EUR45M to Icelandic bank Kaupthing, 26 Sep 2008"*. [Colapso financiero: Análisis de la exposición Confidencial de 205 empresas cada uno sobre el EUR45M al banco islandés Kaupthing] [en línea]
<https://www.wikileaks.org/wiki/Financial_collapse:_Confidential_exposure_analysis_of_205_companies_each_owing_above_EUR45M_to_Icelandic_bank_Kaupthing,_26_Sep_2008> [Consulta: 10/10/2012]
[147] DOMSCHEIT-BERG, op. cit., p. 103
[148] *Idem* y p. 107.

CAPÍTULO II

¿CUÁLES SON LAS FUGAS MÁS IMPORTANTES DE *WIKILEAKS*? ¿CUÁL ES LA RELACIÓN ENTRE *WIKILEAKS* Y LOS MEDIOS DOMINANTES? ¿CUÁL HA SIDO LA REACCIÓN DEL GOBIERNO DE EE.UU.?

II.1. ¿CUÁLES SON LAS FUGAS MÁS IMPORTANTES DE WIKILEAKS?

II.1.1. Abril de 2010: El video "Collateral Murder".

En la mañana del 12 de Julio de 2007 dos helicópteros Apache con cañones de 30 mm volaban sobre la ciudad Iraquí de Bagdad filmando el suburbio por el que ejercían patrullaje.

II.1.1.1. La información y el productor de la información. La información contenida en el video comienza con una vista tomada desde el aire por medio de una cámara blanco y negro instalada en uno de dos helicópteros del ejército estadounidense que realizaban una operación de vigilancia conjunta.

Luego, la cámara enfoca a un grupo de hombres, uno de ellos parece armado, sin embargo, el comportamiento del grupo era tranquilo. El diálogo que se lleva a cabo es el siguiente:

---

[149] DOMSCHEIT-BERG, op. cit., p. 70.

"- (…) hay más que siguen pasando y uno de ellos tiene un arma.

- Entendido. Objetivo quince recibido.

- Ok

- Mira toda esa gente de pie allí abajo.

- Mantente firme (La cámara enfoca al grupo). Mantente firme y abre el patio.

- Sí, recibido. Calculo que hay, probablemente, unos veinte de ellos.

- Hay uno, sí.

- Oh, sí! (La cámara enfoca a Said Chmagh, conductor de *Reuters* portando una cámara).

- Sí, recibido. Elemento *Bushmaster* [control de infantería]. Copia uno-seis.

- Eso es un arma. (Se suma a la toma la distinción dentro del grupo de la figura del fotógrafo Namir Noor-Eldeen portando otra cámara).

- Sí. Hotel 2-6. *Crazy Horse* 1-8 [segundo helicóptero Apache].

- Copia en uno-seis. *Bushmaster* seis Romeo. Recibido.

- *Fucking prick*.

- Hotel 2-6. *Crazy Horse* 1-8 [comunicación entre helicópteros]. Tenemos individuos con armas. Sí, el también tiene un arma. Hotel 2-6. *Crazy Horse* 1-8. Tenemos cinco o seis individuos con *AK47s*. Pedimos permiso para atacar.

- Recibido. Eh, no tenemos personal al este de nuestra posición. Así que, eh, tienes vía libre para atacar. Cambio.

- De acuerdo, vamos a atacar.

- Recibido. Adelante.

- Voy a…no puedo cogerlos ahora porque están detrás de aquel edificio.

- Um, ey tropa *Bushmaster*.

- ¡¿Es eso un *RPG* [lanzagranadas antitanque de mano]?!

- De acuerdo. Tenemos a un tipo con un *RPG*.

- Voy a disparar.

- Ok. No espera, demos la vuelta.

- Detrás de los edificios ahora desde nuestro punto de vista… De acuerdo, vamos a dar la vuelta.

- Hotel 2-6 apunto a un individuo con un *RPG*. Preparándome para disparar. No vamos a…

- Sí, tenemos a un tipo a tiro. Y ahora está detrás del edificio. Maldita sea.

- Eh, negativo, él estaba, eh, justo enfrente del *Brad* [*Bradley Fighting Vehicle*, camión blindado de transporte]. Eh, más o menos ahí, a la una en punto [orientación/dirección]. No he visto nada desde entonces.

- Estupideces. Cuando estés encima de ellos simplemente reviéntalos.

- Ok.

- Veo tu tropa, eh, tengo unos cuatro *Humvees* [vehículos acorazados] alrededor…

- Tienes vía libre.
- De acuerdo. Abro fuego.
- Avísame cuando los tengas.
- Disparemos.
- Préndeles fuego a todos.
- Vamos, ¡fuego! (Comienzan a ametrallar al grupo y se observan nubes de polvareda levantándose.)
- Continúa disparando… continúa disparando… continúa disparando (Los hombres que no han sido asesinados y pueden desplazarse, se dispersan corriendo mientras reciben el fuego abierto. La cámara enfoca a uno de los que huyen y las balas se dirigen hacia él hasta que cae muerto. Se trata de Namir Noor-Eldeen, fotógrafo de *Reuters*).
- Hotel. *Bushmaster* 2-6. *Bushmaster* 2-6. Tenemos que movernos ¡Ahora mismo!
- De acuerdo. Acabamos de atacar a los ocho individuos.
- Sí, vemos dos pájaros [helicópteros] y todavía estamos abriendo fuego [no lo están] (Se aprecia que Said intenta escapar).
- Recibido. Los tengo. (Acribillan a Said)
- 2-6, aquí 2-6. Estamos moviéndonos.
- Ups, lo siento. ¿Qué ocurría?
- Maldita sea Kyle.
- Vale, jajaja, les he dado.
- Vale, despejado.
- Vale, estoy buscando objetivos de nuevo.
-*Bushmaster* 6, aquí *Bushmaster* 2-6… (La gráfica de los editores del video destaca el cuerpo de Said Chmagh en el suelo).
- Tengo un montón de cuerpos tirados ahí.
- Vale, hemos disparados a unos, uh, ocho individuos.
- Sí, tenemos a uno arrastrándose ahí abajo…pero uh, ya sabes, tenemos, definitivamente tenemos algo.
- Estamos disparando unos cuantos más.
- Recibido.
- Hey, tu dispara, yo hablaré.
- Hotel 2-6, *Crazyhorse* 1-8.
- Crazyhorse 1-8, aquí Hotel 2-6. Cambio.
- Recibido. Ahora estamos atacando a ocho individuos aproximadamente…eh, *KIA* [muertos en combate], eh…*RPGs* y *AK-47s*.
- *Hotel* 2-6, tienen que moverse a esa posición en cuanto *Crazyhorse* haya acabado y fotografiarlo. Corto. *6 beacon Gaia*.
- La posición es *Sergeant 20*.
- *Hotel* 2-6, *Crazyhorse* 1-8.
- Oh, sí, fíjate en esos hijos de puta muertos.
- Precioso.
- 2-6, *Crazyhorse* 1-8.

- Precioso.
- Buen tiro.
- Gracias.
- *Hote*l 2-6. *Hotel* 2-6, *Crazyhorse* 1-8.
- *Crazyhorse* 1-8. *Bushmaster* 7. Adelante.
- *Bushmaster* 7. *Crazyhorse* 1-8. Eh, posición de los cuerpos: Mike Bravo 5-4-5-8-8-6-1-7 [referencia a mapa de coordenadas militar].
- Ey, bien en, eh…
- 5-4-5-8-8-6-1-7. Cambio.
- Aquí *Crazyhorse* 1-8, copia buena. Están en una calle en frente de una, eh…plaza descubierta con varios, eh, camiones azules, eh, varios vehículos en la plaza.
- Hay un tipo moviéndose ahí abajo, pero está, eh, está herido.
- Vale, se lo haremos saber para que se den prisa y vayan allí.
- 1-8 también tenemos un individuo, eh, parece estar herido intentando alejarse a rastras. (La cámara enfoca a Said Chmagh moribundo en el suelo tratando de moverse y escapar)
- Recibido. Vamos para allá.
- Recibido. Cesamos el fuego. Sí, no vamos a disparar más.
- Se está levantando.
- ¿A lo mejor tiene un arma bajo su mano?
- No. No he visto ninguna todavía.
- Chicos, veo que cazaron a aquel tipo que se arrastra por la vereda.
- Sí, lo hice. Disparé dos ráfagas cerca de él, y ustedes chicos, estaban disparando ahí también, así que, eh, ya veremos.
- Sí, recibido.
- Tropa *Bushmaster* 30-2; aquí…eh, Hotel 2-7, cambio.
- Hotel 2-7; *Bushmaster* 7 adelante.
- Recibido. Sólo quiero asegurarme de que tienen mi césped [área], cambio.
- Recibido. Tenemos tu césped.
- Vamos, colega. (Se observa como Said Chmagh trata de incorporarse).
- Todo lo que tienes que hacer es coger un arma.
- *Crazyhorse*. Aquí *Bushmaster* 5, *Bushmaster* 4. Cambio.
- Estamos justo debajo de ti. Ahora puedes llevarnos a ese lugar.
- Aquí 2-6 recibido. Lanzaré bengalas. También tenemos a un individuo moviéndose. Estamos buscando armas. Si vemos un arma, atacaremos.
- Sí *Bushmaster*. Tenemos un furgón acercándose y recogiendo los cuerpos.
- ¿Dónde está ese furgón?
- Justo ahí abajo, donde los cuerpos.
- Ok, sí.
- *Bushmaster*, *Crazyhorse*. Tenemos individuos yendo hacia la escena, posiblemente, eh, recogiendo cuerpos y armas.

- Déjame atacar… ¿Puedo disparar?

- Recibido. Corto.

- Eh, *Crazyhorse* 1-8 pidiendo permiso para… eh…atacar. (En este momento ya se ven tres hombres que bajaron de un furgón oscuro a prestarle auxilio a Chmagh y llevarse los cuerpos).

- ¿Recogiendo los heridos?

- Sí. Estamos intentando conseguir permiso para atacar.

- ¡Vamos! ¡Déjennos disparar!

- *Bushmaster*, *Crazyhorse* 1-8.

- Se lo están llevando.

- *Bushmaster*, *Crazyhorse* 1-8.

- Aquí *Bushmaster* 7. Adelante. (las personas que asisten a Said Chmagh logran ingresarlo dentro del furgón).

- Recibido. Tenemos un SUV…eh…furgón bongo negra recogiendo los cuerpos. Pido permiso para atacar.

- ¡Mierda!

- Aquí *Bushmaster* 7, recibido. Aquí *Bushmaster* 7, recibido. Ataquen. (El furgón comienza muy lentamente a avanzar sin estar todos los ocupantes dentro de él, buscar reenfilarse en el camino para salir de ahí.)

- 1-8. Atacando. Despejado.

- ¡Vamos! (Vuelven a dispararse los cañones ahora contra el furgón y sus ocupantes. Los dos ocupantes que estaban fuera del furgón alcanzan a reaccionar de la ráfaga y corren hacia las paredes)

- Despejado (Nuevas ráfagas de ametralladora dirigidas contra los que huían a refugiarse en unas paredes y contra el furgón, cuyo conductor en su desesperación retrocede y choca con las paredes hacia las que habían huído otros de sus pasajeros).

- Despejado.

- Estamos atacando. (Tercera tanda de ráfagas de ametralladora).

- Nos acercamos. Vía libre.

- Recibido. Estamos intentando… eh…

- Despejado.

- Les oigo ven…Les he perdido entre el polvo.

- Los tengo.

- Estoy disparando.

- Aquí *Bushmaster* 40 tienes algún BDA [estimación de daños en combate] sobre esa furgoneta. Cambio.

- Tienes vía libre. Aquí, eh…*Crazyhorse*. Espera.

- No puedo disparar por alguna razón.

- Adelante.

- Creo que el furgón está deshabilitado.

- Adelante y dispárale.

- Tengo un bloque con el acimut por alguna razón. [artillero movió la mirilla demasiado lejos]. (Nueva ráfaga de disparos).

- A la izquierda. (Otra ráfaga de ametralladora).

- Izquierda despejada. (Otra ráfaga).

- De acuerdo *Bushmaster*, *Crazyhorse* 1-8. Un vehículo parece estar neutralizado. Había aproximadamente cuatro o cinco individuos en el vehículo trasladando cuerpos. El Bradley más adelantado debería tomar la próxima a la derecha. Eso es cruzando al este por la carretera. Nos más disparos.

- *Crazyhorse* aquí *Bushmaster* 4. Estamos moviendo tropa [infantería] hacia el sur entre los *Bardleys* [tanques].

- Tengo tu tropa…eh, la tropa Bradley, moviéndose al sur por la carretera donde tuvo lugar el combate.

- Última llamada a la estación…eh, tropa Bradley, repita.

- Recibido. Aquí *Crazyhorse*. Su Bradley principal acaba de girar al sur, por la carretera, donde han sucedido todos los ataques. Debería tener un furgón en medio de la carretera con unos doce o quince cuerpos.

- ¡Ey! ¡Mira eso! ¡Justo en el medio del parabrisas!

- ¡Ja, ja!

- Vale, había… aproximadamente de cuatro a cinco individuos en ese camión, así que estoy contando de doce a quince.

- Yo diría que hasta ahora es una estimación bastante correcta.

- Recibido.

- Sólo quiero que me aconsejen, 6, *Bushmaster* 6 está montándolos ahora mismo."[150]

En el video editado por *WikiLeaks*, las imágenes de la cámara del helicóptero se interrumpen para exponer el texto que dice que ocho minutos después de la acciones las tropas llegan al escenario.[151] También se muestra la siguiente declaración: "Nos detuvimos, paramos, y les oí decir por el *intercom* que no condujeran los Bradley por ahí, ya que había demasiados cuerpos y no querían pasarles por encima." Capitán James Hall, capellán castrense (*Washington Post*)".[152]

Vuelven las imágenes de la cámara del Apache y así también los diálogos:

[150] http://www.collateralmurder.com/
[151] *Idem*.
[152] *Idem*.

"(Inmediatamente se ve un tanque pasando por el lugar en el que ocurrieron los hechos por encima de un cuerpo)

-Me parece que ha pasado por encima de un cuerpo.

- ¿De verdad?

- (Risas) ¡Sí!

- Tal vez fue sólo una ilusión óptica, pero parecía. (El video en este momento retrocede y hace un zoom en la imagen demostrando que la eventual ilusión óptica no había ocurrido.)"

Nueva pausa en la toma aérea. Se lee el siguiente texto: "Los soldados encontraron dos niños heridos en la furgoneta.

Eventualmente un soldado trató de evacuar a los niños al centro médico de la cercana base americana de *Rustamiyah*. Sin embargo, órdenes de mando superior requirieron que los entregaran a la policía iraquí y fuesen atendidos en un hospital iraquí.

Esto significaría una asistencia médica demorada y considerablemente peor."

Vuelven las imágenes suministradas por la cámara del Apache y se observa ahora como un grupo de soldados estadounidenses recorren el lugar.

La comunicación entre los soldados que sobrevuelan Irak y las tropas sigue de la siguiente manera:

"- ¡Eh! Necesito los *Brads* para eliminar a los extremistas. Tengo una niña herida, hay que llevarla a *Rustamiyah*.

- *Bushmaster* 7. Hotel 2-6. ¿Quieres que nos movamos a tu ubicación? Corto.

(…)

(Soldados avanzan hacia los vehículos y uno de ellos corre llevando sobre sí la niña denominada #1.)

- *Bushmaster* 6. *Hotel* 2-6. Cambio.

- Hotel 2-6; Aquí *Bushmaster* 7. Recibido, ven a nuestra ubicación.

- Ok, recibido, vamos hacia el norte en *Gandins* y de ahí iremos al este hasta tu localización.

(Posteriormente se ve a un soldado estadounidense corriendo y sosteniendo en sus brazos al "niño #2" y se sube con él a un vehículo.).

(… Corte de la continuidad del video)

- Recibido. Negativa a la evacuación de dos...eh, civiles…eh, niños, al…eh, hospital militar. Van a tener que hacerse cargo los *IP* [policía iraquí]. Ellos pueden asistirnos en esto. Corto. Los *IPs* los trasladarán a un hospital local, cambio.

- Copiado, cambio.

- Recibido. Uno seis oh.

(… Corte de la continuidad del video)

(…)

- Bueno, es culpa suya por traer a sus niños a una batalla.

- Es verdad."[153]

La imagen sobrevolando es interrumpida por el siguiente texto:

"No hay asesinatos deliberados de civiles inocentes por nuestra parte. Hacemos grandes esfuerzos por impedirlo. Sé que dos niños resultaron heridos e hicimos todo lo posible por ayudarles. Ignoro cómo pudieron resultar heridos." Mayor Brent Cummings. Oficial ejecutivo 2-16 del ejército de Estados Unidos. (*Washington Post*)".

Vuelve a mostrarse una toma desde el aire y muestran el momento antes a que la furgoneta fuera ametrallada. Se trata de una toma del helicóptero que envía las ráfagas de ametralladora y que es acompañado por el helicóptero desde el cual observamos los hechos el tiempo anterior. Pues bien, se da cuenta claramente que desde el helicóptero se podía perfectamente distinguir que dentro del vehículo había la presencia de dos menores mirando desde la ventana del copiloto hacia el exterior mientras los adultos hacen lo posible por rescatar y sacar de ahí a Said Chmagh.

La secuencia de imágenes se interrumpe para exhibir el texto que sigue:

"Cuando resultó que asesinaron a Namir, se nos contó que había efectuado un bombardeo aéreo una hora antes y que dos periodistas habían muerto". Nos relata Ahmad Sahib, un fotógrafo de France – Presse que iba en

[153] *Idem.*

auto unos bloques detrás de Noor-Eldeen y que estaba hablando con él a través del celular cuando lo asesinaron."

Luego continúa el testimonio de Sahib:

"Llegaron, bajaron del auto y empezaron a tomar fotos mientras la gente se reunía. Parecía que los helicópteros americanos tuvieran intención de disparar porque en el momento de salir de mi auto y empezar a tomar encuadres mientras la gente se reunía uno de los helicópteros disparó varias ráfagas contra unos edificios cercanos y corrimos para ponernos a cubierto". Ahmad Sahib, fotógrafo de guerra de AFP (*The New York Times*)."[154]

Luego se realiza una dedicatoria del video a las familias de las personas asesinadas en este ataque y a todas las víctimas de guerra de las que se desconocen sus circunstancias. Finalmente, se presentan los créditos.[155]

En total en aquel incidente murieron doce personas y dos niños resultaron heridos. La historia de la mayoría de los asesinados nos es desconocida, pero sí conocemos las de dos de ellos, dos empleados inocentes de la agencia *Reuters*: Said Chmagh y Namir Noor-Eldeen. Chmagh tenía cuarenta y cuatro años y era conductor y auxiliar de *Reuters*[156] dejando a su mujer y cuatro hijos[157]. Noor-Eldeen era fotógrafo de guerra y tenía veintidós años[158], era considerado uno de los mejores fotógrafos de todo Irak y provenía de una familia de periodistas.[159] .

Los militares estadounidenses afirmaron que todos los muertos eran insurgentes o fuerzas "anti-iraquíes" que se produjeron en una batalla. "No hay duda alguna de que la Coalición ha entrado en combate con una fuerza hostil"

[154] *Idem*.
[155] *Idem*.
[156] LEIGH y Harding, op. cit., p. 82.
[157] http://www.collateralmurder.com/
[158] LEIGH y Harding, op. cit., p. 82.
[159] http://www.collateralmurder.com/

dijo el T. Coronel Scott Bleichwehl portavoz del ejército de Estados Unidos en Bagdad (*The New York Times*).”[160]

Reuters exigió una investigación por los asesinatos. “Las autoridades militares concluyeron que las acciones de los soldados y pilotos involucrados se ajustaban al Derecho en Conflictos Armados y a sus Reglas de Entrenamiento”.[161]

En agosto de 2007 *Reuters* solicitó una copia de la videoevidencia tomada por el helicóptero responsable del ataque. El video nunca fue liberado.[162]

Los productores de la información son pilotos del ejército estadounidense que en julio de 2007 comandaban un par de helicópteros Apache AH-64 mientras sobrevolaban un suburbio de Bagdad a mil metros de altitud.[163]

II.1.1.2. La fuente. Assange no proporcionó ninguna información acerca de la procedencia del video sin editar, sólo que lo obtuvo de la memoria caché de “fuentes militares”.[164] En su biografía no autorizada habría dicho: “Nuestras estructuras de denegación (…) no permiten en absoluto saber si Bradley Manning era la fuente de alguno de los materiales que habíamos difundido. Nuestros servidores no proporcionan esta clase de información, ni siquiera yo podría obtenerla.[165]„

¿Quién es Bradley Manning? Es un analista de inteligencia del Ejército de Estados Unidos que fue detenido el 26 de mayo de 2010 bajo la acusación de ser responsable de filtrar el video *Collateral Murder* publicado por *WikiLeaks*.

---

[160] *Idem*.
[161] *Idem*.
[162] *Idem*.
[163] LEIGH y Harding, op. cit., p. 82.
[164] *Idem*, p. 83.
[165] O´HAGAN, op. cit., p. 213 - 214.

Los cargos incluyen ocho violaciones de ley y cuatro violaciones del código interno del Ejército[166].

Manning tuvo acceso a la *SIPRNET*, del Departamento de Defensa, también usado por el Departamento de Estado como la parte del sistema de red centralizada de diplomacia llevado a cabo en respuesta a las recomendaciones de la Comisión 9/11.[167]

El soldado, en unas presuntas conversaciones mantenidas en mayo de 2010 a través de la Internet con el *hacker* norteamericano Adrian Lamo, habría admitido que sustrajo y entregó a *WikiLeaks* cientos de miles de documentos secretos, con la voluntad manifiesta de cambiar el mundo. Lamo filtró estos *chats* inicialmente a la revista *Wired* y delató a Manning ante el *FBI* y el Ejército. Tomó esa decisión, según dijo, por temor a que el soldado pusiera en riesgo la seguridad nacional norteamericana. Estas supuestas conversaciones son ahora un indicio que obra en manos de la fiscalía militar, que además ha seguido el rastro de Manning en los ordenadores portátiles de la base de Hammer, en Irak. El equipo de abogados de Manning no ha confirmado ni desmentido la autenticidad de esos contactos.[168]

Manning reivindica la protección de denunciantes. La complejidad de esta cuestión se puso de manifiesto en rueda de prensa del 29 de noviembre de 2005. El Secretario de Defensa, Donald Rumsfeld, dijo que los soldados estadounidenses no tienen la obligación de detener activamente los actos de tortura realizados por autoridades iraquíes sino simplemente informarla. Sin embargo, el general Peter Pace, quien también estuvo presente, no estuvo de acuerdo respondiendo que "es absolutamente responsabilidad de cada

[166] MAURER, op. cit., p.12, referencia n° 60.
[167] *Idem*, p. 12.
[168] EL PAIS,"*Enterrando al soldado Manning"*. Madrid, 20 de marzo de 2011. [en línea] <http://elpais.com/diario/2011/03/20/domingo/1300596753_850215.html> [Consulta: 01-09-2012]

miembro del servicio de EE.UU., si ve que un trato inhumano se está llevando a cabo, intervenir para detenerlo".[169]

Sin embargo, Manning no parece haber aprovechado la protección a la denuncia de irregularidades señaladas en el Código Militar de los EE.UU. No limitó las fugas a lo que él creía acciones ilegales. Por esta razón, a juicio de profesor Joseph Nye, Manning no es un denunciante, debido a la gran cantidad de material liberado siendo en su mayoría no susceptible de beneficiarse con la protección de denuncia de irregularidades.[170]

Además, según el profesor Benkler, no existe duda de que el gobierno puede someter a proceso a sus propios empleados, especialmente aquellos cuyo trabajo se relaciona con la seguridad nacional, tengan acceso a información clasificada debido a su empleo y revelen este material clasificado. En concreto, Manning fue acusado en virtud de las siguientes disposiciones: primero, la Ley de Espionaje en su sección 793 (e), la cual prohíbe a cualquier persona voluntariamente comunicar "cualquier documento (...) relativo a la defensa nacional, y que "se tenga razones para creer que esta información podría ser utilizada para la lesión de los Estados Unidos o en beneficio de cualquier nación extranjera"; segundo, la Ley 18 USC § 952, que prohíbe específicamente la divulgación de cables diplomáticos; y, finalmente, la Ley de Fraude y Abuso Informático en sus secciones 1030 (a) (1) y 1030 (a) (5) al excederse en su acceso autorizado a computadoras del gobierno.[171]

Finalmente, el 21 de agosto de 2013 Manning fue condenado a 35 años de prisión, 10 años más que el plazo en que los mismos documentos que él filtró serán desclasificados y habiéndose excluido el cargo de ayuda al enemigo. La justicia militar estadounidense dictó la sentencia con la sanción más extensa

[169] MAURER, op. cit., p.13, referencia n° 67.
[170] *Idem*, p. 13.
[171] BENKLER, Yochai. *"A free irresponsible press: Wikileaks and the battle over the soul of the networked fourth estate"*. Harvard Civil Rights-Civil Liberties Law Review, 2011, p. 43.

con que jamás se haya castigado una fuga de información, quedando pendiente el recurso de apelación[172].

II.1.1.3. El editor. A fines de marzo de 2010 ya en Islandia Assange se dispuso a arrendar una casa y editar el video. David Leigh, redactor jefe del equipo de investigación del *The Guardian* intentó proponerle un trato para hacer público el video. Assange le dijo que le avisaría algo, pero nunca lo hizo.[173]

El periodista inglés estaba informado de la futura filtración porque ambos estuvieron invitados la semana anterior a una conferencia en Noruega para celebrar el vigésimo aniversario de una activa asociación de periodismo. Esa misma noche después de la cena Assange le hizo ver reservadamente las imágenes.[174]

Al parecer, más tarde Assange habría llegado a un acuerdo periodístico con el *The New Yorker.* En los hechos, su redactor Raffi Khatchadourian, seguía al fundador de *WikiLeaks* para hacerle un perfil que apareció publicado en el mes de Junio. En el intertanto de la edición del video en análisis, tuvo la posibilidad de tomar notas al momento de llegar un mensaje desde Bagdad que entregaba mayor información sobre las víctimas mostradas en las imágenes.

Escribió: “Los periodistas que fueron a Bagdad […] localizaron a los dos niños del furgón. Los niños vivían a una manzana del lugar del ataque, y aquella mañana su padre los llevaba al colegio. 'Recuerdan el bombardeo, sufrieron un dolor enorme, dicen, y perdieron la conciencia', escribió uno de los periodistas […].

Jönsdottir se volvió hacia Gonggrijp, a quien se le habían hinchado los ojos: '¿Estás llorando?', le preguntó.

---

[172] THE GUARDIAN, *“Bradley Manning: a sentence both unjust and unfair”*. [Bradley Manning: Una sentencia injusta y desleal] 21 de agosto de 2013 [en línea] <http://www.theguardian.com/commentisfree/2013/aug/21/bradley-manning-sentence-unjust> [Consulta: 24-08-2013]

[173] LEIGH y Harding, op. cit., p. 85.

[174] *Idem*, p. 81.

'Sí, sí – respondió-. Vale, vale, es eso de los niños, es doloroso.'

Gonggrijp se recompuso: '¡Maldita sea!', dijo […]. Ahora a Jönsdottir también se le caían las lágrimas y se sonaba la nariz."

Finalmente, el 5 de abril, el video titulado *Collateral Murder,* fue presentado en el *National Press Club* en Washington, DC., para ser visto más de 12 millones de veces en *Youtube*.

Las personas que trabajaron directamente, como se puede extraer de los créditos que se mencionan en el video, fueron:

"sus valerosas fuentes; Julian Assange como director y productor creativo; Rop Gonggrijp como coproductor; Alan D.B. como ingeniero jefe e investigador; Kristinn Hrafnsson como desarrollador de la historia; Ingi Ragnar Ingason como editora visual e investigadora y, Birgitta Jonsdottir como coproductora y guionista."[175]

II.1.1.4. La audiencia. El video causó revuelo, pero no la indignación universal ni la presión de reformas que consiguió la filtración periodística de impacto mundial inmediatamente anterior. Hablamos de la publicación del *The New Yorker* de fotos en que se veían prisioneros iraquíes siendo humillados y torturados. Se menciona como factores de este resultado primero, a la falta de participación activa de *Reuters* en la protesta pública ante la revelación de asesinatos de dos de los suyos y, segundo, a lo tendencioso del título que se decidió adjudicar a las imágenes, pues de cierta manera la audiencia rechaza que se la condicione *ex ante*.[176]

II.1.1.5. ¿Por qué es importante? Primero, porque produce en el espectador un intensa Identificación con las víctimas, humanizándolo. Así, lo ayuda a sopesar el horror de una ocupación y la toma de decisiones que se toman sobre otras vidas. En definitiva, es capaz de transportar a la audiencia al lugar en que se libra la ocupación, graficando vivamente la cruel decisión de

[175] http://www.collateralmurder.com/
[176] LEIGH y Harding, op. cit., p. 86 - 87.

tratar las calles de una ciudad como un campo de batalla en el cual todas las personas son blancos fáciles, y genera un debate tanto acerca de los actos de violencia realizados, como de la complicidad de otros a través de su ocultamiento.

Ello no habría tenido lugar de no ser por la fuente que envió el material a *WikiLeaks* decidiendo que tenía que verse, y de no ser por la decisión de Assange de confrontarlo con la luz pública. Es razonable pensar que a partir de entonces, el asesinato de civiles provocado tan comúnmente por soldados estadounidenses desde el aire, tendrá un tratamiento un poco menos frívolo por parte del público estadounidense.[177]

II.1.2. Julio de 2010: Los Afghan War Diaries.

II.1.2.1. La información y el productor de la información. El material estaba compuesto por 90.000 documentos del puesto de mando central de las fuerzas armadas de los Estados Unidos. Entre ellos figuran informes de situación, informes sobre tiroteos y ataques aéreos, datos sobre incidentes sospechosos y los llamados *threat reports* (informes de amenazas).[178]

La noche del 17 de Junio de 2007, cinco misiles impactaron con gran estruendo contra una escuela religiosa en Afganistán, reduciéndola a escombros. Después de aterrizar los helicópteros de asalto comprobaron que habían matado a siete niños.[179]

El servicio de información del comando de operaciones especiales del ejército de estadounidense describió lo ocurrido de la siguiente forma:

"**Ataque aéreo en *Paktika***

[177] *Idem*, p. 87.
[178] DOMSCHEIT-BERG, op. cit., p. 163.
[179] LEIGH y Harding, op. cit., p.135.

AERÓDROMO DE *BAGRAM*, Afganistán.

Fuerzas afganas y de coalición llevan a cabo una operación en el distrito de Zargun Shah, en la provincia de *Paktika*, que ha tenido como resultado la muerte de varios extremistas y civiles y la detención de dos extremistas. Información creíble de inteligencia había señalado el complejo, que comprendía una mezquita y una madraza (escuela religiosa), como presunto refugio de guerrilleros de *al-Qaeda*.

Las fuerzas de coalición habían confirmado la presencia de actividades violentas ocurridas en el emplazamiento antes de obtener la aprobación para llevar a cabo el ataque cerero sobre el mismo. Después del ataque, los residentes en el complejo confirmaron la presencia de combatientes de al-Qaeda durante todo el día.

La primera información [sugiere que] siete niños de la madraza murieron como resultado del ataque. 'Es un ejemplo más de la utilización que hace *al-Qaeda* de las ventajas protectoras de las mezquitas, y también de los civiles inocentes, a quienes utiliza como escudo –dijo Maj Chris Belcher, del ejército, un portavoz de la *Joint Task Force*-82 -. Estamos apesadumbrados por las vidas inocentes que se han perdido por culpa de la cobardía extremista'".[180]

El diario destapó que en realidad no hubo ataque aéreo, sino que un ensayo de un potente e indiscriminado nuevo sistema de misiles guiados por *GPS* que podían dispararse desde la carga de un camión a 65 kms. de distancia. Además, no fueron "fuerzas afganas y de coalición" ordinarias, sino que por una brigada de asesinos estadounidenses llamados *Task Force* 373 que trabajaban a partir de una lista de dos mil personas a la que tenían la orden de asesinar, añadiéndose personas a la lista sin ningún tipo de control judicial. Si le desagradabas a un gobernador de Afganistán, te nominaba y al cabo de unos minutos esa persona oía el zumbido del motor de un helicóptero y su casa era bombardeada.[181]

[180] *Idem*, p.135 - 136.
[181] O´HAGAN, op. cit., p.224.

Finalmente se devela que la detección de “actividades violentas” en el lugar no era su motivación, sino que la esperanza de que el comandante *Al Libi* estuviera allí.[182]

“El diario de guerra filtrado da la siguiente información [las abreviaturas has sido desarrolladas]:

Fecha 17-06-2007, 21.00.00
Tipo Acción amiga
Título 172100Z[ulu time] T[ask] F[orce] 373 OBJ[etivo]

Resumen
NOTA: La siguiente información (TF-373 e HIMARS) está clasificada como secreta / *NOFORN* [*Not for Release to Foreign Nationals*]. El conocimiento de que TF-373 llevó a cabo un ataque con *HIMARS* tiene que mantenerse protegido. Toda la información que sigue está clasificada como secreta / REL[ease] ISAF. [*International Security Assistance Force*]

Misión
S[pecial] O[perations] T[ask] F[orce] lleva a cabo ataque cinético seguido de un ataque de Fuerza de A[salto] con H[elicóptero] para matar / capturar a *ABU LAYTH AL LIBI* en la C[itada] Á[rea de] I[nterés] 2.

Objetivo
Abu Layth Al Libi es un veterano mando militar de *al-Qaeda*, jefe del *LIFG* (Grupo Armado Libio Islámico). Tiene su centro de operaciones en *Mir Ali*, Pakistán, y dirige campos de entrenamiento por todo el norte de *Waziristán*. La vigilancia a lo largo de la pasada semana indica una concentración de árabes en los alrededores de la zona del objetivo.

Resultado
6 X E[nemigos] M[uertos] E[n[C[ombate] (EKIA); 7 x N[o] C[ombatientes] KIA [muertos en combate] 7 X detenidos

Resumen
La Fuerza de Asalto en Helicóptero (*HAF*) parte de la base de Orgun-E para llevar a cabo un enlace y posicionamiento frente al objetivo inmediatamente después del fuego anterior al asalto. Por orden, se lanzan cinco cohetes y se destruyen estructuras en el objetivo (*NAI* 2). La *HAF* traslada rápidamente la fuerza de asalto a la *HLZ* (zona de aterrizaje del helicóptero). La

[182] LEIGH y Harding, op. cit., p.136 - 137.

ISR (la vigilancia de inteligencia) informa de múltiples varones no identificados huyendo de la zona de objetivo. La fuerza de asalto se despliega rápidamente por la zona objetivo y establece estrategia de contención por el lado sur del objetivo. Durante el asalto inicial, las fuerzas aéreas descubren a varios *MAM* (varones en edad militar) escapando de la zona de objetivo. El mando de las fuerzas de tierra (*GFC*) calcula 3 *EKIA* huyendo al norte y 3 *EKIA* huyendo al sur del complejo, neutralizados por fuego aéreo. La fuerza de asalto maniobra rápidamente con un elemento *SQUAD* (escuadrón) con el resto de fugados. El elemento captura a 12 *MAM* y regresa a la zona de objetivo. El *GFC* pasa a una evaluación inicial de 7 *NC KIA* (niños). Durante los interrogatorios oficiales se evalúa que a los niños no se les ha permitido salir del edificio debido a la presencia de *UIM* (hombres sin identificar) en el complejo. La fuerza de asalto pudo recuperar un *NC* niño entre los escombros. El equipo médico le retira rápidamente los restos de la boca y le práctica maniobras de resucitación cardiopulmonar durante veinte minutos. Debido a las restricciones de tiempo, el jefe de la *TF* pone en acción un elemento de Fuerza de Reacción Rápida contra un objetivo posterior (*NAI* 5). Controlan rápidamente el objetivo e inician el asalto. El objetivo es asegurado y la fuerza de asalto tiene inicialmente 6 *MAM*. El GFC recomienda que se detenga a 7 *MAM* para practicar interrogatorios adicionales. El *TF CDR* considera que la fuerza de ataque continuará SSE. El gobernador ha sido informado de la situación actual y solicita ayuda para acordonar la zona de operaciones con el apoyo de la policía nacional afgana y las fuerzas de coalición locales en busca de un Individuo de Gran Valor. Un Equipo de Reconstrucción Provincial está de camino a la zona de operaciones.

1.- El objetivo era un veterano jefe de *al-Qaeda*.

2.- Se llevaron a cabo reconocimientos del patrón cotidiano del 18 de junio desde las 08.00 hasta las 18.15 (hora del ataque) sin indicación alguna de presencia de mujeres o niños en el objetivo.

3.- La mezquita no era un objetivo ni fue atacada; informes iniciales indican que no ha sufrido daños.

4.- Un anciano que estaba en la mezquita declaró que los niños fueron retenidos contra su voluntad e intencionadamente en el interior del recinto.

ACTUALIZACIÓN: 18 0850Z Junio 07

- El gobernador *Khapalwak* no ha logrado todavía ponerse en contacto con el presidente *Karsai* (debido al horario tan ocupado del presidente hoy), pero espera poder hablar con él en una hora. (P[residente] d[e] A[fganistán] contactado más avanzada la tarde aprox. 14.00Z.)
- El gobernador hizo una *shura* [consulta] esta mañana a la que acudieron [autoridades] locales de los distritos de *Yahya Yosof* y *Khail*.
- Habló de los puntos de discusión que se le había facilitado y añadió unos cuantos propios que coincidían con nuestra actual narración.

> - El ambiente de la población *[sic]* local es que están en estado de shock, pero comprenden que el incidente fue provocado en realidad por la presencia de vándalos.
> - La gente piensa que es bueno que se matara a hombres malos.
> - La gente lamenta la pérdida de vidas de niños.
> - El gobernador se hizo eco de la tragedia de los niños muertos, pero insistió en que se podía haber evitado si la gente hubiera denunciado la presencia de insurgentes en la zona.
> - El gobernador promete otra *shura* dentro de unos días y que las familias serán compensadas por sus pérdidas.
> - Al gobernador se le preguntó cómo están los ánimos de la gente y respondió: 'La operación ha sido buena y la gente se cree lo que le hemos dicho.'" [183]

Este informe grafica el tipo de documentos que salieron a la luz en esta publicación.

Además, se obtuvo información acerca de uso excesivo de la fuerza contra civiles por parte de unidades del ejército británico. Un destacamento de los *Coldstream Guards* de reciente ubicación en *Kabul* describía en un diario no oficial que el ambiente era amenazante por la existencia de hombres bomba, cuyos ataques ya se habían sufrido. En cuatro ocasiones esa unidad disparó a civiles de la localidad con el fin de protegerse. El peor caso es el del 21 de octubre de 2007, cuando soldados estadounidenses informaron de un caso de fuego amigo en el centro de *Kabul*, describiendo que tropas desconocidas dispararon a un vehículo civil ocupado por tres intérpretes además del conductor. Informaron que las tropas iban en un "vehículo de tipo militar de color marrón, con un artillero arriba", descartando la presencia y también la implicación de estadounidenses. Al actualizar el mensaje escribieron: "LA INVESTIGACIÓN ESTÁ CONTROLADA POR LOS BRITÁNICOS. NO NOS ES

[183] *Idem*, p.137 a 139.

POSIBLE OBTENER TODA LA INFORMACIÓN. ESTE CASO PERTENECE A LAS FUERZAS ISAF BRITÁNICAS."[184]

Después de la publicación tuvieron que pasar tres meses de maniobras dilatorias para que el Ministerio de Defensa en Londres admitiera que estos hechos habían ocurrido. La patrulla británica mató a un civil e hirió a otros dos que iban en un minibús plateado aludiendo infructuosas advertencias de detención.[185]

El 6 de noviembre de 2007, los británicos informaron que habían herido a otro civil al mediodía. En la tarde los estadounidenses oyeron que el hombre había muerto y que era el hijo de un general de la aviación afgana.[186]

El ejército británico acabó confirmando la filtración de *WikiLeaks* al cabo de largo tiempo, aludiendo nuevamente infructuosas advertencias de detención.[187]

Estos hechos y otros cientos muy parecidos constituyen la historia oculta de la guerra de Afganistán, en que constantemente morían inocentes a manos de soldados extranjeros.[188]

Los productores de la información son los miembros de la Coalición de ejércitos establecidos en Afganistán, especialmente el estadounidense e inglés con las actividades de sus unidades *Task Force* 373 y *Coldstream Guards,* respectivamente.

II.1.2.2. La fuente. Los 92.000 informes fueron supuestamente entregados a Assange por el soldado estadounidense Bradley Manning.[189]

---

[184] *Idem*, p.142.
[185] *Idem*.
[186] *Idem* p.142 y 143.
[187] *Idem*, p.143.
[188] *Idem*.

II.1.2.3. El editor. WikiLeaks obtuvo el material y fue publicado en todo el mundo por el *The Guardian* (13 páginas[190]) y sus socios *The New York Times* (8 páginas[191]*)* y *Der Spiegel* (17 páginas[192])[193], publicándose por primera vez el 25 de julio de 2010[194]. David Leigh de *The Guardian* fue quien llevó la batuta.[195]

The Guardian publicó la información *online*, el periódico neoyorquino lo esperó, pues no se atrevió a ser el único medio en publicarlo para el mercado de EE.UU. *Der Spiegel* llamaba continuamente a los miembros de *WikiLeaks* para saber cuando publicarían en la Internet. Hubo cierto caos del que el mundo exterior no sabía.[196]

Los periódicos europeos se enfocaron en el sufrimiento de los civiles[197]. El periódico alemán escogió para su portada el título "La guerra secreta de Estados Unidos" haciendo mención a los actividades del escuadrón *Task Force* 373[198]-[199]. El periódico inglés por su parte, profundizó en la lista de 2.000 objetivos que debía "matar o capturar" aquel escuadrón[200].

El periódico estadounidense "al parecer no tuvo los suficientes bríos para publicarla"[201] y optó por dar un enfoque más estratégico de la guerra en Afganistán. Se centró en estudiar la gran cantidad de pruebas que demostraban

---

[189] *Idem*, p.136.
[190] O´HAGAN, op. cit., p.227.
[191] *Idem*.
[192] *Idem*.
[193] LEIGH y Harding, op. cit., p.136.
[194] *Idem*, p.140.
[195] DOMSCHEIT-BERG, op. cit. p. 218.
[196] *Idem*, p. 162.
[197] LEIGH y Harding, op. cit., p.143.
[198] *Idem*, p.140.
[199] O´HAGAN, op. cit., p.224.
[200] LEIGH y Harding, op. cit., p.140.
[201] O´HAGAN, op. cit., p.224.

que los esfuerzos estadounidenses por eliminar a los talibanes eran obstaculizados por Pakistán.[202]

Por primera vez en mucho tiempo aquellos tres periódicos se situaron en la primera línea del debate generado en torno a la verdadera naturaleza de la guerra moderna.[203]

II.1.2.4. La audiencia. En la primera oleada de los medios se habló bastante del contenido examinado por ellos. En la segunda, los medios que no habían accedido a la primicia realizaron sus análisis. Pero finalmente se inició en todo el mundo un debate sobre la posibilidad de que aquella publicación hubiera podido perjudicar a alguien.[204]

II.1.2.5. ¿Por qué es importante? Ningún periódico, libro o película había podido facilitar hasta entonces informaciones tan concretas, y además, de primera mano, sobre la guerra de Afganistán.[205]

Por primera vez se revelan detalles de misiones letales realizadas por la *Task Force* 373 y otras unidades, que se ocultaban tras una pared de desinformación, planteando el debate acerca de la legalidad de las matanzas y de lo confinamientos a largo plazo sin juicio. Además, plantea un cuestionamiento sobre tácticas en que ineludiblemente se matará y herirá a ciudadanos inocentes. [206]

II.1.3. Octubre de 2010: Los documentos de Irak War Logs.

II.1.3.1. La información y el productor de la información. 391.832 documentos liberados a la vez que cubrieron desde el 1º de enero de 2004 al

[202] LEIGH y Harding, op. cit., p.143.
[203] O´HAGAN, op. cit., p.227.
[204] DOMSCHEIT-BERG, op. cit. p. 169.
[205] *Idem*, p. 163.
[206] LEIGH y Harding, op. cit., p.140.

31 de diciembre de 2009. Estaban constituidos por los informes que los soldados norteamericanos habían realizado dando cuenta de los incidentes que les habían parecido dignos de ser mencionados. En las redacciones se pueden leer todos los detalles: lugar exacto, día y hora, unidades militares participantes, cifra de muertos y si estos eran norteamericanos, aliados, tropas iraquíes, insurgentes o civiles[207]:

"EL VEHÍCULO SALIÓ DE LA CARRETERA Y CAYÓ A UN CANAL A 1,5 KM AL NORTE DE *SAQLAWIYAH* (38S LB768976) Y SE HUNDIÓ. (1) HOMBRE ADULTO SALIÓ DEL VEHÍCULO Y FUE RECUPERADO DEL CANAL; LOS DEMÁS PASAJEROS SE HUNDIERON CON EL VEHÍCULO. EL HOMBRE ADULTO FUE TRATADO POR EL AYUDANTE MÉDICO EN EL MISMO LUGAR Y FUE TRANSPORTADO AL *JCC* DE *SAQLAWIYAH* Y MÁS TARDE TRANSPORTADO AL HOSPITAL JORDANO. EL S(ERVICIO) DE LA P(OLICÍA) I(RAQUÍ) DE *SAQLAWIYAH* ACUDIÓ A LA ESCENA Y RECUPERÓ (2) MUJERES ADULTAS, (3) NIÑOS DE ENTRE 5 Y 8 AÑOS Y (1) BEBÉ DEL VEHÍCULO. TODOS (6) SE HABÍAN AHOGADO. EL *SPI* DE *SAQLAWIYAH* LLEVARÁ TODOS LOS CUERPOS RECUPERADOS A RAMADI." [208]

El arriba expuesto es un informe filtrado que describe como los marines dispararon contra el parabrisas de un auto a veinte metros de distancia, quizás "demasiado" cerca de un convoy de suministros a las afueras de Bagdad. [209]

Es representativo de la publicación de los diarios de guerra de Irak, pues contiene hechos que describen, primero, fuego en contra de civiles y, segundo, el conteo específico de los muertos.

Otro caso es el de noviembre de 2005, en que los marines estadounidenses lanzaron la Operación Telón de Acero en la ciudad de *Husaybah* y sus alrededores, cerca de la frontera con Siria. Luego de diecisiete días de combate el Pentágono publicó una nota de prensa que tituló "Ha concluido la Operación Telón de Acero que se desarrolló en la frontera entre

[207] O´HAGAN, op. cit., p. 244.
[208] LEIGH y Harding, op. cit., p.152 - 153.
[209] *Idem*, p.153.

Irak y Siria" siendo colgada en la *web* de las fuerzas norteamericanas. El informe declara que "los oficiales informaron de la muerte de 10 marines durante Telón de Acero. En la operación cayeron muertos 139 terroristas en total y 256 fueron arrestados". Fechada el 22 de noviembre de 2005, no menciona víctimas civiles.

El informe filtrado, que lleva la fecha de 11 de noviembre de 2005 dice:

"[la patrulla] de apoyo de Telón de Acero informó haber encontrado cadáveres civiles enterrados en tres sitios diferentes de *Husaybah*. En [el primer sitio] fueron recuperados los cuerpos de 3 mujeres, 3 hombres y un niño. En [el segundo] se recuperaron 7 mujeres y 10 niños. En [el tercero] 1 niño no pudo ser recuperado…Todos los cadáveres fueron identificados sin lugar a dudas por los vecinos, y el padre del niño que no pudo ser recuperado lo identificó como hijo suyo. Todas las víctimas fueron recuperadas en zonas atacadas por los aviones de combate aliados el 7 de noviembre de 2005".[210]

"Nosotros no contamos los muertos", fue la frase acuñada en 2002 por el general Tommy Franks, un año antes de dirigir la invasión norteamericana a Irak, la que se convirtió en un mantra silencioso de Bush y de Blair.[211]

Se había comunicado diligentemente que 4.748 soldados estadounidenses y aliados habían muerto hasta la navidad de 2010, mientras, al mismo tiempo, aseguraron durante años que no había otras estadísticas oficiales referidas a las víctimas.[212]

La publicación de octubre de 2010, de una enorme base de datos referida a incidentes y muertos, desmiente las declaraciones oficiales. Los documentos exhiben un "registro detallado, incidente por incidente, de 66.081 muertes violentas, por lo menos, de civiles iraquíes durante la invasión"[213] La cifra es de suyo gigantesca, pero dado el espacio temporal cubierto, aun es

[210] O´HAGAN, op. cit., p. 240.
[211] LEIGH y Harding, op. cit., p.147.
[212] *Idem*, p.148.
[213] *Idem*, p.147.

posible suponer que sea baja. La base de datos comienza en 2004, un año después del comienzo de la guerra, y acaba el 31 de diciembre de 2009. Es más, no tenemos datos acerca de las muertes civiles causadas directamente por actividades militares.[214] Por ejemplo, en la ciudad de *Fallujah* hubo dos grandes batallas en 2004 que la redujeron casi a escombros. Los documentalistas del ejército no recogen ni una sola muerte de civiles. En otros casos, el ejército de EE.UU. mató a civiles pero los registró erróneamente como enemigos. Tal es el caso del registro de los empleados de *Reuters* asesinados por el helicóptero Apache.[215]

Una posterior investigación realizada por *Irak Body Count* (dedicada durante años a contar cadáveres inadvertidos) ONG filial del *Oxford Research Group*, mejoró los números crudos y estadísticamente sucios, llegando a la conclusión, a finales de 2010, que el total absoluto de muertes civiles documentadas por la violencia en Irak está entre 99.383 y 108.501. Por lo tanto, el conteo de víctimas o muertos hechos públicos por la coalición, solo nos mostraba un porcentaje ínfimo de la realidad.[216]

II.1.3.2. La fuente. Según el gobierno de Estados Unidos, Bradley Manning sería la fuente.[217]

II.1.3.3. El editor. El 22 de Octubre de 2010 el material pasó a estar disponible para todo el mundo en la página *WikiLeaks*. Como en los diarios de guerra de Afganistán, *The Guardian, The New York Times* y *Der Spiegel* pudieron revisar el material y escribir sus propios artículos semanas antes de la

[214] *Idem*, p.148.
[215] *Idem*.
[216] *Idem*, p.149 y 150.
[217] *Idem*, p.148.

publicación. Sin embargo ahora también habría otros socios a bordo, los canales de televisión *Al-Jazeera* y *Channel 4*[218]*.*

En esta publicación quien llevó la batuta fue Gavin MacFadyen, director del *Centre for Investigative Journalism* de Londres. Assange lanzó la publicación en el *Hotel Park Plaza* junto con la ONG *Irak Body Count*, un equipo de filmación de documentales y un miembro de *Public Interest Lawyers*.[219]

II.1.3.4. La audiencia. Se generó un interés presencial mayor por parte de la prensa al generado en el lanzamiento de los documentos afganos. Acudieron unos 300 periodistas para difundir además la noticia al resto del mundo. [220] La respuesta moral a la liberación de los diarios de Irak fue similar a la reacción con los diarios de Afganistán, pero los medios fueron más críticos respecto a la información revelada.[221]

II.1.3.5. ¿Por qué es importante? Los gobiernos de los Estados Unidos y del Reino Unido se habían negado a declarar cuántos civiles iraquíes habían muerto durante el proceso de guerra y ocupación argumentando su inexistencia, lo cual fue probado falso por la publicación de *WikiLeaks*.

Luego se pudo hacer una estadística basada en los documentos y posteriormente se pulieron los datos por la ONG *Irak Body Count*, para llegar a impactantes cifras de civiles muertos.

Además, otro análisis de datos, realizado por Nick Davies de *The Guardian*, reveló que Irak sigue siendo una cámara de tortura en la que se arresta, maltrata y asesina como si Saddam nunca hubiese sido derrocado.[222] Así, tras haberse revelado la colusión de las tropas norteamericanas con las

[218] DOMSCHEIT-BERG, op. cit. p. 218.
[219] LEIGH y Harding, op. cit., p.153.
[220] *Idem*, p.153.
[221] MAURER, op. cit., p. 32, referencia n° 238.
[222] LEIGH y Harding, op. cit., p.150.

torturas infligidas a cientos de presos iraquíes por parte de las fuerzas locales, el ministerio de defensa de Dinamarca comenzó una investigación para analizar el comportamiento de las tropas de su país en Irak. En un principio se solicitó información no editada al Pentágono, que se negó. Luego, se lo pidieron a *WikiLeaks*, que se los facilitó.

Los historiadores futuros podrán mensurar si todo ello contribuirá a que las futuras aventuras militares estadounidenses y británicas sean menos sanguinarias.[223]

Para el fundador de *WikiLeaks*, los diarios de guerra de Afganistán y de Irak "han contribuido de forma crucial a la comprensión de esas guerras. Revelan de qué forma se produjeron los diversos incidentes sobre el terreno, y además sirven para poner al mundo en alerta respecto al modo en que las informaciones oficiales sobre los mismos tendían a quitarles hierro, tanto cuando esas informaciones procedían de las fuerzas armadas como cuando eran reproducidas por los medios de comunicación. Una y otra vez se minimiza o falsea el número de víctimas civiles (…)"[224].

Por mucho que el Pentágono se empeñe en publicitarlo, la guerra moderna no se limita al fuego archipreciso, sino que trae consigo los mismos desastres de sangre, tragedia e injusticia que desde siempre han supuesto las guerras.

II.1.4. Noviembre de 2010. La mayor filtración de la historia. Los telegramas diplomáticos.

II.1.4.1. La información y el productor de la infrmación. 251.287 cables escritos por 280 embajadas y consulados en 180 países diferentes. De los documentos un 40 por ciento estaban clasificados como confidenciales y un 6

[223] *Idem*, p.149.
[224] O´HAGAN, op. cit., p. 238.

por ciento eran secretos. No había ninguno de categoría alto secreto, pues ese material ultraconfidencial se omitía de la base de datos *SIPRNET*, además, y paradójicamente, las mejores historias procedían de aquellos con una confidencialidad más baja[225].

Había evaluaciones francas y con frecuencia no se dedicaban a halagar a los líderes mundiales. La mayoría, análisis de buena calidad contrastando con la parquedad de los diarios militares. Ponían de relieve los intereses y preocupaciones de la única superpotencia, pero más importante que eso, incluyen revelaciones acerca de asuntos que los ciudadanos tanto estadounidenses como de otros países tienen derecho a saber: espionaje corporativo, cuentas bancarias ocultas, abusos contra los derechos humanos, corrupción, vínculos dudosos entre los líderes del G8.[226]

El principio de selección y publicación declarado por *The Guardian* era el del interés público, lo que quedaría de manifiesto en la difusión del cable de julio de 2009 que revela que el gobierno de Estados Unidos espiaba a la Organización de las Naciones Unidas y a su secretario general, *Ban Ki–moon*. El cable comienza solicitando información diplomática sobre las posiciones acerca de temas candentes como Afganistán, Darfur, Somalia, Irán y Corea del Norte, pero leído con atención se ve claramente desdibujado el límite entre diplomacia y espionaje.[227]

Washington pedía información sensible de las comunicaciones, como contraseñas o claves cifradas, información biométrica detallada sobre agentes clave de Naciones Unidas, así como información secreta sobre el estilo de gestión y toma de decisiones de *Ban Ki–moon*. También quería números de

[225] LEIGH y Harding, op. cit., p.202 - 203.
[226] *Idem*, p.235.
[227] *Idem*, p.235 y 236.

tarjeta de crédito, direcciones de correo electrónico, números de teléfono y de fax.[228]

Esta "directiva nacional para recopilar inteligencia humana" se distribuyó por todo el mundo además de las misiones de Estados Unidos en Naciones Unidas. Viena, Roma y 33 embajadas y consulados, incluyendo Londres, París y Moscú, a la totalidad de las agencias de inteligencia norteamericanas y al Departamento de Estado.[229]

La publicación y conocimiento de este cable tuvo como efecto que el portavoz del secretario general de la ONU enviara una carta recordando a los Estados miembros la inviolabilidad de las Organización de las Naciones Unidas.[230]

Otros cables de interés público fueron los que revelaron la presión constante que ejerció el rey Abdulá de Arabia Saudita para lograr que Estados Unidos atacara a Irán para destruir su programa nuclear, al igual que otros aliados árabes, lo que ni siquiera se sospechaba.[231]

También quedó de manifiesto la preocupación de Israel por conservar su monopolio nuclear regional y su disposición para atacar unilateralmente a Irán, además de sus intentos por influir en Washington. [232]

El caso Yemení es patético, se revela la participación encubierta de Estados Unidos en Yemen acordada con el presidente de ese país en virtud del cual el país árabe haría pasar como propios ataques de los americanos contra al-Qaeda. El primer ataque contraterrorista ocurrió en diciembre de 2009 y mató

[228] *Idem*, p.236.
[229] *Idem*.
[230] *Idem*, p.237.
[231] *Idem*..
[232] *Idem*.

a docenas de civiles junto con presuntos militares. El gobierno de Yemen lo presentó como actuación propia con ayuda de inteligencia estadounidense.[233]

Pero el punto más impresionante fue Rusia. Los cables dejan a la luz pública que con frecuencia es difícil allí distinguir entre las actividades del gobierno y la del crimen organizado. Tráfico de armas, blanqueo de dinero, enriquecimiento personal, protección de gángsters, extorsión, maletas llenas de dinero y cuentas secretas en paraísos fiscales. Se calcula que en ese país los sobornos alcanzan los 300.000 millones de dólares al año. De muestra un botón: los organismos encargados del orden público, policía, agencias de espionaje y la Fiscalía, dirigen de facto una organización protectora de redes delictivas, es más, otros cables dicen abiertamente que controlan la red de crimen organizado del país.[234]

Se publicó a través de los documentos que la corrupción de la burocracia rusa es tan alta que maneja un sistema tributario paralelo para el enriquecimiento privado de la policía, el funcionariado y el sucesor de la *KGB*. Además, durante años ha corrido el rumor de que Putin amasa personalmente una fortuna secreta fuera del país y que ha llegado a acuerdos secretos sobre energía con el ex primer ministro italiano, Silvio Berlusconi.

También se reveló que los rusos enviaban armas a los kurdos para desestabilizar Turquía y estaban detrás del caso de un carguero sospechoso de llevar misiles a Irán.

En relación con China, se dio cuenta de una relación insospechadamente displicente con Corea del Norte, la que comenzó a gestarse con las pruebas nucleares de este último país. Pekín indica que está incluso dispuesta a la reunificación de Corea, y en secreto, se distanciaba de su secreto aliado.

---

[233] *Idem*, p. 238.
[234] *Idem*, p. 239 - 240.

Otro punto importante de las revelaciones tuvieron que ver con el caso Megrahi, que desde 1988 constituía un problema diplomático estadounidense, libio, inglés y finalmente hasta escocés. Su denominación se debe al nombre del agente de la inteligencia libia encarcelado por haber participado en el famoso atentado contra un avión.[235]

En 2009, Megrahi fue puesto en libertad por Reino Unido, supuestamente por razones humanitarias debido a un cáncer prostático que lo tenía al borde de la muerte. Esta decisión iba en dirección opuesta a los deseos de EE.UU. pues varios de sus ciudadanos murieron en el atentado. Un año más tarde, el agente seguía vivo después de haber sido recibido como un héroe en Trípoli.[236]

El cable filtrado revelaría una verdad bastante diferente en las motivaciones de la liberación del libio. El documento era de autoría de Richard Le Baron, encargado de negocios de Londres, fechada el 24 de octubre de 2008. Señalado como PRIORIDAD tanto por el secretario de Estado en Washington como por el Departamento de Justicia, el cable estaba clasificado como *CONFIDENTIAL//NOFORN* y empezaba así:

"Convicto terrorista Pan Am 103 Abdelbasset al-Megrahi tiene cáncer inoperable, incurable, pero no está claro cuánto le queda de vida".[237]

Los cables recogían una presión creciente de Libia sobre los británicos, estos últimos tendrían que sopesar entre el eventual enojo de los estadounidenses y las amenazas de represalias comerciales de Gadafi si Megrahi llegase a morir encarcelado. La solución que encontraron fue trasladar

[235] *Idem*, p.161.
[236] *Idem*.
[237] *Idem*

la decisión al gobierno autónomo de Escocia, cuyos dirigentes se quejaron ante Estados Unidos de que no habían obtenido nada del acuerdo.[238]

Los documentos mostraban a los británicos como unos inútiles, pues con toda su supuesta influencia no consiguieron evitar la portentosa bienvenida propia de un héroe y se retorcían ante la posibilidad de un funeral apoteósico basados en información falsa de que Megrahi estaba a punto de morir.[239]

También, develaban que Estados Unidos daba en el gusto a ambas partes. Por un lado dejaban que los políticos descargaran su ira contra la perfidia libia, y, por otro, el departamento de Estado señalaba que se podían aunar esfuerzos con Gadafi para derrotar a *al-Qaeda*. [240]

Gadafi por su parte se dejaba llevar por rabietas cuando en Naciones Unidas no lo dejaron levantar su icónica tienda. Motivó incluso notas para calmarlo firmadas por Hillary Clinton para que Libia siguiera desmantelando su supuesto arsenal nuclear ante las amenazas del extinto gobernante negándose a enviar de vuelta a Rusia un avión cargado con uranio enriquecido. Los expertos estadounidenses advertían aterrados la inminente amenaza radiactiva de tener un contenedor de uranio sin vigilancia durante un mes.[241]

Los cables muestran una superpotencia engatusando, maniobrando y a veces, intimidando, las actitudes demenciales de Gadafi y las limitadas opciones abiertas al Reino Unido pese a sus pretensiones de ocupar un lugar más alto en el mundo.[242]

En lo que concierne más propiamente con el Reino Unido, los cables claramente incomodan. Los estadounidenses evalúan a la familia real con un

[238] *Idem*, p.162.
[239] *Idem*.
[240] *Idem*, p.163.
[241] *Idem*.
[242] *Idem*.

cómico desdén. Aunque ese tono se perdía cuando se referían a los aliados del Reino Unido, estos últimos, quienes anhelaban una "relación especial"[243].

La superpotencia estaba interesada en sus propias prioridades: quería usar ilimitadamente las bases militares británicas, que los políticos del Reino enviaran tropas para sus guerras y que compraran armas y productos comerciales de Estados Unidos. En concordancia con ello, el encargado de negocios norteamericano en Londres recomendó seguir consintiendo las fantasías británicas sobre su especial relación.[244]

Los cables hacen posible distinguir con cruda realidad quién es el socio mayor y quién el menor. Cuando el ex secretario de Exteriores británico, David Miliband, intentó obstaculizar los vuelos espía de Estados Unidos desde la base en Chipre, fue devuelto rápidamente a su lugar. Y cuando Gordon Brown, como primer ministro, solicitó personalmente un indulto a Gary McKinnon, un joven *hacker* del que se pedía extradición, su pedido fue desoído de modo humillante.[245]

Otras historias de mucho interés fueron la de los 25 millones de dólares pagados en sobornos a políticos de la India; las interferencias norteamericanas en la política interna de Haití; presiones de la diplomacia norteamericana a favor de empresas estadounidenses; pagos de políticos lituanos a periodistas para mejorar su imagen pública, etc.[246]

---

[243] *Idem*, p.244 – 245.

[244] "Aunque es tentador decir que tener a *HMG* [El gobierno de Su Majestad] inseguro de su actual posición con nosotros podrías hacer que Londres estuviera mejor dispuesto a reaccionar favorablemente cuando se le presiona para que preste ayuda, a la larga no es de interés para Estados Unidos que la población del R.U. llegue a la conclusión de que la relación se está debilitando por ambos lados. La asignación de recursos del Reino Unido – financieros, diplomáticos, militares – en apoyo de las prioridades globales de Estados Unidos sigue sin tener paralelo."Richard LeBaron, encargado de negocios norteamericano en Londres. LEIGH y Harding, op. cit., p. 245.

[245] Idem, p.245 – 246.

[246] O´HAGAN, op. cit., p. 266.

Pero los cables no sólo tratan acerca de lo que Estados Unidos veía, sabía y opinaba de otros Estados, sino que también de algunas de las mayores empresas del mundo que han estado vinculadas a dudosas prácticas.

En relación a la gigante de los hidrocarburos *Shell*, aparece que su vicepresidente para el África Subsahariana hacía alarde de haber ubicado con éxito a su gente en los principales ministerios del gobierno de Nigeria, estando bien enterados para conocer los planes para licitar concesiones de petróleo. Los activistas lo decían hace tiempo, pero los cables lo confirmaban, había conexiones entre el gigante del petróleo y los políticos en un país en que el 70% de la población es pobre.[247]

La farmacéutica más grande del mundo, *Pfizer*, también se vincula a cables provenientes de Nigeria. La empresa era perseguida judicialmente por unos polémicos ensayos con medicamentos para niños con meningitis. Los cables filtran que contrataron detectives para conseguir pruebas de corrupción contra el fiscal general del país. *Pfizer* públicamente dice que no ha cometido delito alguno y que ya ha resulto la denuncia presentada en 2009 por el gobierno de Nigeria y el estado de Kano, donde el medicamento se usó durante un brote de meningitis.[248]

II.1.4.2. La fuente. Se presume por el Gobierno norteamericano que la fuente ha sido Bradley Manning.

II.1.4.3. El Editor. El 28 de Noviembre de 2010 se publicaron los primeros cables en *cablegate.org*, sin embargo sería difícil hablar de los telegramas en un primer momento, pues se tuvo acceso sólo a unos centenares de cables, una ínfima parte, aunque en el futuro los 250.000 documentos iban a ir apareciendo en *cablegate.wikileaks.org*, en pequeñas dosis.

[247] LEIGH y Harding, op. cit., p.247.
[248] Idem.

II.1.4.4. Audiencia. Esta publicación generó un interés inmenso tanto en los medios como en la opinión pública mundial.

II.1.4.5. ¿Por qué es importante? Algunos comentaristas de medios que no participaron de la filtración, afirman que los telegramas no tienen sustancia informativa. A ello bastaría responder con la siguiente pregunta ¿No es de interés público que una potencia mundial como Estados Unidos se dedique a espiar a la ONU de forma sistemática? Con ese sólo informe basta para responder a esa afirmación, y sabemos que han sido varios más los publicados.[249]

Los cables también han sido vistos, por otros comentaristas de medios, como la prueba de que a Estados Unidos le cuesta imponer sus ideas en el mundo, entrando en un largo período de relativo declive. Otros, que se presenta una imagen bastante buena de la burocracia del departamento de Estado quedando impresionados con el profesionalismo del cuerpo diplomático norteamericano.

Lo que sí es indiscutible es que dan una imagen del mundo mucho más nítida que la habitual, un nuevo mapa de la realidad mundial mucho más fidedigno.

En algunos casos, las consecuencias de la filtración fueron rápidas, algunos diplomáticos fueron cambiados de puesto y otros simplemente despedidos. En Enero de 2011, Washington tuvo que retirar a su embajador en Libia, Gene Cretz. Silvia Reed, encargada de negocios en Asjabat que vilipendió con sus opiniones escribiendo un perfil del presidente de Turkmenistán, fue asignada a otro puesto, en Vladivostok.

[249] DOMSCHEIT-BERG, op. cit., p. 236 - 237.

Como consecuencia positivas más concretas, por ejemplo, en un cable de la embajada norteamericana en Bangladesh se demuestra que el gobierno británico entrenaba a una fuerza paramilitar condenada por organismos de Derechos Humanos y conocida como "escuadrón gubernamental de la muerte", vinculada a cientos de muertes extrajudiciales. Al quedar al descubierto por los cables no se han declarado más asesinados.[250]

También se puede hablar del caso tunecino. El cable publicado por el periódico de Beirut *Al-Akhbar* escrito por el embajador Robert Godec en julio de 2009 decía:

"El problema está claro, Túnez ha sido gobernado por el mismo presidente durante veintidós años. No tiene sucesor. Y aunque el presidente Ben Alí merece que se le reconozca el mérito de continuar muchas de las medidas progresivas de (su predecesor) el presidente Burguiba, él y su régimen han perdido el contacto con el pueblo tunecino. No toleran ni consejos ni críticas, sean nacionales o internacionales. De forma creciente, dependen de la política para controlar (el país) y se concentran en conservar el poder (…) Crece la corrupción en el círculo interno. Incluso los tunecinos medios son muy conscientes de ello y el coro de quejas aumenta. A los tunecinos les desagrada, incluso odian a la primera dama, Leila Trabelsi, y a su familia. En privado, los oponentes al régimen se burlan de ella; incluso los que están cerca del gobierno expresan su consternación por su conducta. Mientras la rabia va creciendo ante el alto nivel de desempleo y las desigualdades regionales. Como consecuencia, los riesgos para la estabilidad a largo plazo del régimen van aumentando".[251]

Antes de un mes después de la publicación del cable, Túnez se paralizaba por lo que algunos llaman la primera revolución *WikiLeaks.*[252]

El cuestionamiento más fuerte que sí se le puede aplicar a la publicación de los telegramas diplomáticos y que también la hace importante es el de preguntarse si al entregarse estos papeles secretos, antes información a la que sólo accedía privilegiadamente el ejército y el ministerio de asuntos exteriores

[250] LEIGH y Harding, op. cit., p. 250.
[251] Idem.
[252] Idem.

estadounidense, en exclusiva a cinco grandes medios de comunicación ¿no se estará solamente cambiando quienes son los guardianes de aquellos secretos decidiendo qué debe llegar a la opinión pública y que no? En opinión de Domscheit-Berg, la estrategia de publicación elegida se aleja bastante de la idea original de *WikiLeaks*.[253]

También podemos estar de acuerdo con la afirmación de que las filtraciones de estos cables "levantaban la tapadera que ocultaba muchísimas operaciones secretas, ponían al descubierto prejuicios largamente sostenidos, mostraban casos embarazosos para los países y para las actividades de las personas, y lo hacían en todos los niveles de la actividad gubernamental".[254]

II.2. ¿CUÁL ES LA RELACIÓN ENTRE WIKILEAKS Y LOS MEDIOS DOMINANTES?

II.2.1. ¿Cuáles son los medios dominantes?

Los medios dominantes son aquellos que fijan la pauta de cómo se organizan los medios, de cuál es su estándar ético al procesar y publicar la información. En este proceso de filtraciones, es *WikiLeaks* finalmente quien determina cuales son los tres, y luego los cinco medios más importantes del mundo. Es importante destacar que se trata de medios escritos, pues a ellos

[253] DOMSCHEIT-BERG, op. cit., p. 238.
[254] O´HAGAN, op. cit., p. 263.

Wikileaks les concedería un estatuto de credibilidad que no tiene, por ejemplo, la televisión. [255]

Veamos cuáles han sido los medios escogidos por *WikiLeaks* para trabajar en conjunto para las grandes filtraciones de 2010:

II.2.1.1. The New York Times. Fundado en 1851 y con una larga tradición, es el tercer periódico más grande de su país, detrás de *The Wall Street Journal* y *USA Today*. Siguiendo las tendencias de la industria, su circulación semanal se ha reducido a menos de un millón diario desde 1990. Su sitio online es el más popular de los periódicos de Estados Unidos con más de treinta millones de visitas mensuales. Ha sido considerado desde hace mucho tiempo por la industria nacional como el "periódico de referencia". [256]

En 1971 sirvió de publicación para la anterior filtración más grande de la historia, la de los *Pentagon Papers*, sin duda que esto también debió haber sido determinante para la inclusión que pensó Assange.

La percepción pública lo define mayormente como liberal en distintas encuestas, lo que se deduce por ejemplo por el apoyo al matrimonio igualitario y porque no ha respaldado a un republicano para presidente desde Dwight D. Eisenhower en 1956.[257]

Se decidieron por él ante la filtración de los diarios de guerra de Afganistán. Se argumentan razones estratégicas para contactar con un periódico estadounidense y "¿por qué no con el más importante?"[258]

II.2.1.2. The Guardian. El segundo socio de mayor relevancia para *WikiLeaks* como medio en sí, aunque operativamente ha sido el primero[259], fue

[255] MAGALLÓN, Raúl. *"Wikileaks: ¿Un cambio de paradigma?"*, op. cit., p.128.
[256] http://en.wikipedia.org/wiki/The_New_York_Times
[257] Idem.
[258] DOMSCHEIT-BERG, op. cit. p. 162.

fundado en 1821 en Manchester. *The Guardian* certifica una difusión media diaria de 204.222 ejemplares, en diciembre de 2012. En comparación con las ventas de 547.465 para *The Daily Telegraph*, 396.041 para *The Times* y *The Independent* con 78.082.[260]

Una encuesta de 2005 muestra que el 48% de sus lectores eran votantes laboristas y un 34% votantes del Partido Liberal Demócrata, por lo que la principal corriente política lectora del periódico es la izquierda británica.[261]

Se identifica actualmente con el liberalismo social. En las últimas elecciones generales del Reino Unido en 2010, apoyó a los demócratas liberales, que formaron un gobierno de coalición con los conservadores.[262]

Julián Assange decía contar con buenos contactos en el periódico.[263] De hecho, tuvieron relación antes, en una de las primeras filtraciones de *WikiLeaks*. Además, pensaba que quienes defienden las causas justas gustan de este periódico, como por ejemplo, su fidelidad a la verdad tras los acontecimientos del 11 de septiembre de 2001, su persecución a políticos corruptos y su información sobre los horrores de la guerra.[264]

II.2.1.3. El País de España. Fundado en 1976, su promedio de tiraje a 2010 es de 473.407 ejemplares y el promedio de difusión de 370.080, lo que le convierte en el periódico no deportivo de mayor difusión de España. Además tiene una edición global que se imprime y distribuye en América Latina. [265]

Se sostiene que su ideología es demócrata y europeísta. Ha apoyado la figura del Rey Juan Carlos por su contribución a la estabilización democrática

---

[259] Idem.
[260] http://en.wikipedia.org/wiki/The_guardian.
[261] Idem.
[262] Idem.
[263] DOMSCHEIT-BERG, op. cit. p. 162.
[264] O´HAGAN, op. cit., p.216.
[265] http://es.wikipedia.org/wiki/El_País

española, ha criticado al Che Guevara por su determinación a la lucha armada. También se ha mostrado crítico con los últimos gobiernos de Brasil, Argentina y muy especialmente con el del venezolano Hugo Chávez.[266]

II.2.1.4. Der Spiegel. En español "El Espejo", es la mayor revista semanal de Europa y la más importante de Alemania. Su primera publicación data de 1947 y tiene una difusión de un millón de ejemplares semanales.[267]

Desde que Stefan Aust tomó su control en 2002, al semanario se le percibe moviéndose hacia la derecha política, pasando desde apoyar al gobierno eco-socialista a mantener una tendencia neoliberal.[268]

También ha sido acusado por algunos académicos de albergar un sesgo pro-Israel.[269]

El responsable de relacionarse con este medio fue el portavoz de *WikiLeaks* de la época, Domscheit-Berg.[270]

II.2.1.5. Le Monde. Su primera edición data de 1944 coincidiendo con la liberación de Francia de la ocupación nazi.[271] Se informa una difusión media de 323.039 ejemplares por número en 2009, cerca de 40.000 de los cuales se venden en el extranjero.[272]

Su línea editorial es cercana al centro izquierda moderada[273]

II.2.2. ¿Por qué decide cooperar con ellos en 2010?

[266] Idem.
[267] http://es.wikipedia.org/wiki/Der_Spiegel
[268] Idem.
[269] Idem.
[270] DOMSCHEIT-BERG, op. cit. p. 162.
[271] http://es.wikipedia.org/wiki/Le_Monde
[272] Idem.
[273] Idem.

Las filtraciones anteriores habían atraído la atención de los principales medios de comunicación, que comenzaron a buscar activamente a *WikiLeaks*. Assange mismo, por otro lado, había tratado de ganarse esta atención.

Algunos *hacktivistas* ven a estos grandes medios de comunicación como parte del *establishment*. Esto se relaciona con alguna descripción del *The New York Times* que da fe de que contacta al gobierno antes de publicar una historia, que "los periodistas del *The New York Times* tienen un gran y personal interés en la seguridad del país "[274] y que su principal corresponsal en Washington ha señalado que "a veces los periodistas se acercan demasiado a los funcionarios de gobierno"[275].

Así que si *Wikileaks* es en primer lugar un proyecto de medios de corriente crítica ¿Por qué cooperó con medios vinculados al *establishment*?

Hay tres razones principales para que *WikiLeaks* decidiese cooperar con ellos.

II.2.2.1. Capacidad. En primer lugar, se trata de una cuestión de capacidad. Los más grandes medios tradicionales tienen el personal y la experiencia para manejar y redactar una gran cantidad de documentos. [276]

II.2.2.2. Protección. En segundo lugar, el trabajo con medios de comunicación proporciona una cierta protección. Hay una serie bien establecida de precedentes judiciales que tratan acerca de los grandes medios de comunicación y la Primera Enmienda, de los cuales no se ha esclarecido si

[274] MAURER, op. cit, p. 17, referencia 101.
[275] Idem, referencia102.
[276] "(…) esta difusión debían hacerla medios de comunicación convencionales que dispusieran de sus propios equipos de investigación y sus propios redactores, de manera que todos esos materiales adquiriesen un sentido y fueren clarificados. Jamás pretendimos ser capaces de comprender, y ni siquiera nos creímos con capacidad para llegar a leer, todos y cada uno de los documentos contenidos en esos enormes alijos (…) Nosotros solos nos veríamos excedidos por el volumen de todos esos materiales, ya que estábamos hablando de unos 90.000 diarios de guerra de Afganistán, y de 400.000 documentos de Irak". O´HAGAN, op. cit., p.218.

WikiLeaks podría invocarlos. Específicamente, antes de la liberación del *Cablegate*, Assange dijo: "Tenemos que sobrevivir a esta publicación", siendo la razón por la que no hubo una conferencia de prensa y, sobretodo, por la que se previó que los medios de comunicación tradicionales fueran los que lo difundieran primero.[277]

II.2.2.3. Impacto. El objetivo de lograr el máximo impacto político podría lograrse mejor, no sólo a través de una cantidad sin precedentes de material filtrado, sino también a través de una cooperación sin precedentes entre cinco de las más grandes publicaciones del mundo. Podría también interpretarse como un intento de ganar legitimidad, pero dada la cultura *hacktivista* que impregna la ideología *WikiLeaks*, finalmente los medios tradicionales fueron bastante importantes por su efecto multiplicador de fuerza.[278] [279]

II.2.3. ¿Por qué los medios dominantes cooperaron con WikiLeaks?

Para nadie es un misterio que la industria ha estado en crisis en los últimos años. El personal se ha reducido de forma masiva y se han cerrado periódicos en el todo el mundo. Por tanto, hay una intensa competencia entre los medios de comunicación por las historias exclusivas. Si bien la Internet es global, los mercados de los medios siguen siendo predominantemente nacionales. El competidor principal del *The New York Times* es el *The Wall Street Journal*. Contraparte del *Der Spiegel* es el *Der Stern*. Forjar una alianza mundial entre sí dando a cada participante una ventaja competitiva en sus mercados domésticos permitió reducir esta competencia. Trabajar con

[277] MAURER, op. cit., p. 17, referencia n° 105.
[278] Idem, p. 17.
[279] "Nosotros siempre habíamos pensado que los materiales sobre Afganistán e Irak debían ser difundidos a través de varias publicaciones reconocidas. Nos parecía la manera adecuada de hacerlo. En este caso no se trataba de un solo documento y una sola historia, sino de un montón de historias y de cientos de miles de documentos. Habíamos llegado a la conclusión de que esos materiales sólo iban a tener el impacto necesario si eran publicados de manera ambiciosa." O´HAGAN, op. cit., p.218.

WikiLeaks dio a los periódicos "exposición masiva", en otras palabras, ingresos.[280]

Cuando algún colaborador de *WikiLeaks* se contactó por primera vez personalmente con alguno de los cinco grandes medios, lo hizo con *Der Spiegel*, a través de su portavoz alemán de la época, Domscheit-Berg[281]. *Der Spiegel* había tomado nota de *WikiLeaks* después de que lanzó una fuga en relación con los servicios secretos de Alemania y un posterior intercambio de correos electrónicos con Uhrlau, su Director[282]. Pero seguramente luego de la publicación de Asesinato Colateral lograron la atención necesaria para que se interesaran en ellos. Assange se reunió por primera vez con los periodistas de *Der Spiegel* en Londres en julio de 2010.[283]

Con *The Guardian* ya habían tenido una experiencia exitosa en 2007 cuando filtraron el saqueo fiscal del antiguo presidente de Kenia, Daniel Arap Moi, que había ocultado cientos de millones de dólares en cuentas de más de treinta bancos extranjeros distintos[284]. Pero Nick Davies sólo conoció a Assange en Bruselas a finales de junio de 2010. [285]

The Guardian trajo al *The New York Times* convirtiendo en tripartita la alianza periodística. El País de España y *Le Monde* se unieron en el *Cablegate*.[286]

II.2.4. ¿Cómo se dio esta relación?

[280] "El sitio *web* de *The Guardian*, por ejemplo, registró 4,1 millones de usuarios únicos el día del *Cablegate*, el más alto de su historia, al igual que el precio en que sus tarifas de publicidad han sido calculados" MAURER, op. cit., p. 18, referencia n° 110.
[281] DOMSCHEIT-BERG, op. cit., p. 162.
[282] MAURER, op. cit., p. 18, referencia n° 111.
[283] Idem, referencia n°112.
[284] LEIGH y Harding, op. cit., p. 15 y 16.
[285] MAURER, op. cit., p. 18, referencia n° 113.
[286] LEIGH y Harding, op. cit., p. 197.

Antes de relacionarse con los cinco grandes medios, *WikiLeaks* ya tenía ciertas experiencias coordinación de filtraciones y la relación con otros medios, algunas más alentadoras que otras.

La organización fue aprendiendo qué asuntos interesaban más a la prensa y con qué periodistas debían trabajar para que la noticia recibiera la mayor atención posible. También entendieron que era preferible entregar cierta información en exclusiva a algunos periodistas para que la procesaran y la hicieran más digerible para el gran público. [287]

Sin embargo, también entendieron que los medios actúan según su conveniencia ofreciendo a veces sólo pinceladas o pequeñas informaciones seleccionadas, por lo que en definitiva ellos tendrían que publicar íntegramente las informaciones.[288]

Luego de la filtración de Asesinato Colateral, hubo encuentros y desencuentros con los medios norteamericanos, especialmente con el *The New York Times*, pues según Assange "se ven a sí mismos como portadores de la antorcha de lo que ellos creen que son los intereses de su país."[289]

Su estrategia de publicación cambió para la filtración de los diarios de guerra de Afganistán. Se trataba ahora de documentos y de una cantidad altísima, por lo que debían estar más atentos a mantener el control, para así involucrar a los medios en el momento preciso.[290]

Debido a que la filtración de documentos sería gigantesca y, además, relacionada con una guerra en la que Estados Unidos estaba involucrado, sería

[287] DOMSCHEIT-BERG, op. cit., p. 50 y 52.
[288] Idem, p. 52.
[289] LEIGH y Harding, op. cit., p.205.
[290] DOMSCHEIT-BERG, op. cit., p. 162.

estratégicamente necesario involucrar al *The New York Times* y a otros dos grandes medios de comunicación.

Uno de los grandes medios involucrados tempranamente en las grandes filtraciones fue el *The Guardian*, lo que provocó un gran impacto cuando se supo, aunque, como ya sabemos, ya habían trabajado junto a *WikiLeaks* en 2007. En junio de 2010 se reunió Nick Davies, del *The Guardian,* con Assange, para convencer a este último de que la noticia sobre un enorme tesoro de documentos militares y diplomáticos tendría más impacto y significado si pactaban con uno o dos periódicos "por muy tradicionales, cobardes o comprometidos que podamos parecer a los ojos de algunos hackers". Llegaron a acuerdo, naciendo una colaboración excepcional entre, en un principio, tres periódicos y *WikiLeaks*.[291]

En el mismo momento de llevar a cabo la filtración de los diarios afganos, si bien la idea en *WikiLeaks* era que los tres medios publicaran simultáneamente, tampoco les habría importado demasiado que fuera el *The New York Times* el que se hubiese adelantado un poco. Creían que ello podría servir para proteger a sus fuentes, pues era menos probable que el gobierno de Estados Unidos se dirigiera contra el prestigioso periódico, además de que "el hecho de que fuera un periódico estadounidense también dificultaba que las autoridades presentaran cargos de espionaje"[292]. Sin embargo los de Nueva York preferían que fuera *WikiLeaks* el primero en publicar para ellos aparecer como meros reproductores de la información. Esta y otras actitudes comenzaron a mermar la valoración de la relación por parte de los filtradores.[293]

Si bien el vínculo se mantuvo de manera cordial, la manera de funcionar de los medios en su afán de conseguir exclusivas, el intento constante de

[291] LEIGH y Harding, op. cit., p. 18 y 19.
[292] Idem, p. 118.
[293] O´HAGAN, op. cit., p.224 - 225.

sacarles el máximo partido posible y “la mezcla de curiosidad permanente y amistosa autosuficiencia”, a veces sacaba de sus casillas a los integrantes de *WikiLeaks*.[294]

Además, según Assange, pudieron comprobar finalmente hasta qué punto los directores del medio norteamericano está enganchado a la verdad oficial que emite el gobierno[295] y que la ansiedad había mermado a *The Guardian* y a *The New York Times*, pues habiendo tenido lo que querían deseaban proyectar su imagen como la de un *hacker* inestable, intentando apoderarse de todo el mérito y alejarse de posibles acciones judiciales.[296]

En la narración acerca de la filtración sobre el conflicto en Irak, Domscheit-Berg deja entrever que se abrieron nuevos caminos en la forma de negociar con los medios. De hecho, se sospecha que profesionales cercanos a quien dirigió esa publicación (Gavin McFadyen) habían recibido dinero desde *Al-Jazeera* y *Channel* 4 por cinco minutos de videos sobre la guerra de Irak.[297]

Con el paso del tiempo los desacuerdos se tornaron cada vez más graves, sobretodo con el director del *The New York Times*, Bill Keller, quien según Assange estaba empeñado en restar importancia a su papel en las revelaciones y, en una actitud aun más grave, tildándolo de un hombre “para el que la sexualidad es violación y pasatiempo a la vez”[298].

Pero es en la filtración de los cables diplomáticos que surgen grandes confrontaciones entre Assange y *The Guardian/The New York Times.*

[294] DOMSCHEIT-BERG, op. cit. p. 170.
[295] O´HAGAN, op. cit., p.209.
[296] Idem, p.228.
[297] DOMSCHEIT-BERG, op. cit., p. 219 - 220.
[298] O´HAGAN, op. cit., p.232.

Con los ingleses porque estos pretendían publicar telegramas específicos sin el consentimiento del líder de *WikiLeaks*.[299] Al parecer, lo que *The Guardian* deseaba, era publicar los documentos incluso prescindiendo de Assange. Y esto, porque los habían ya conseguido de la periodista Heather Brooke, que a su vez, los había sacado del disco duro de los colaboradores islandeses de *WikiLeaks*. Ello justificaba la furia Assange, sus intentos por retomar el control de la situación a través de su abogado apostado en las oficinas del diario londinense, y explicaba la rapidez del desencadenamiento de la filtración, algo inexplicable e irracional en un principio para el ex vocero de *WikiLeaks*.[300]

Cuenta Assange que antes de publicar los cables, en el desarrollo de la filtración se "debían atender ciertas consideraciones legales, y resolver aspectos importantes relativos a la protección de nuestras fuentes"[301]. Declara que solicitó el compromiso de no publicar nada hasta que él diera luz verde, pero *The Guardian* quería forzarlo a publicar pronto aduciendo que la competencia también tenía una copia de los cables. Se trataba de la periodista del *The Independent* de que hablaba Domscheit-Berg.[302] Finalmente y después de largas y reñidas conversaciones, pudieron disponer de un mes más para poder ordenar los cables.[303]

También hubo grandes discordancias con los estadounidenses, sobretodo porque con anterioridad publicaron un artículo bastante crítico del australiano. Assange declara que la manera en que ya había participado *The New York Times* en el apoyo a las filtraciones había sido lamentable, y que, sumándose a una supuesta hostilidad contra él, hacían que la colaboración perdiera sentido. De hecho, los estadounidenses terminaron participando

[299] DOMSCHEIT-BERG, op. cit., p. 220.
[300] Idem, p. 226.
[301] O´HAGAN, op. cit., p. 266.
[302] Idem.
[303] Idem, p. 272.

también de la exclusiva sólo porque *The Guardian* les hizo llegar el material, quienes a su vez tampoco querían aparecer solos en el contexto anglófono en caso de que surgieran controversias legales. [304]-[305]

Para los periódicos tampoco fue fácil trabajar con Assange, para los británicos "cuando gusta actúa como fuente de filtraciones. Cuando le conviene, se disfraza de editor o de organización de noticias", diciendo que muchos problemas fueron provocados porque la posición de Assange era a veces confusa: a veces fuente, a veces intermediario, a veces editor.[306]

II.2.5. ¿Cómo determinaron que los documentos no eran falsos?

La primera pregunta a la que *WikiLeaks* y los medios de comunicación tradicionales se enfrentaron fue la autenticación.

II.2.5.1. En las publicaciones previas a las grandes filtraciones de 2010. Cada vez que alguien amenazaba a la organización y les exigía que eliminaran inmediatamente un documento de la página *web*, su respuesta consistía en preguntar al requirente si podía atestiguar que poseía el *copyright* del documento. Muchos enviaban una captura de pantalla para probar que detentaban los derechos sobre los documentos. Entonces, se publicaba también esa captura de pantalla, agradeciendo secretamente la facilitación del trabajo.[307]

En otros casos la situación se hacía aun más fácil:

"Para: wikileaks@jabber.se
De: leitungsstab IVBB-BND-BIZ/BIZDOM

[304] DOMSCHEIT-BERG, op. cit., p. 228.
[305] Al *The Guardian* le preocupaba ser el único en obtener y publicar los cables porque la embajada estadounidense en Londres podría intentar emitir un requerimiento de prohibición, pues Reino Unido tiene una de las legislaciones de medios más hostiles del mundo. Necesitaba de una alianza multijurisdiccional. LEIGH y Harding, op. cit., p. 114
[306] Idem, p. 21.
[307] DOMSCHEIT-BERG, op. cit. p. 59 – 60.

Fecha: 16/12/2008 01:15PM
Asunto: Informe clasificado del Servicio de Inteligencia Alemán.

Muy distinguidos señores, en su página web permiten la descarga de un informe clasificado del Servicio de Inteligencia Alemán. Por la presente les solicito que anulen dicha opción de inmediato. He dado ya instrucciones para que se determinen las posibles consecuencias delictivas.

Cordialmente, Ernst Uhrlau

Director del Servicio de Inteligencia Alemán.

De: wikileaks@jabber.se
Para: leitungsstab@bnd.bund.de
cc: wl-office@sunshinepress.org, wl-germany@sunshinepress.org
Fecha: Mar, 18 Dic 2008 09:35:54
Asunto: Re: WG: Informe clasificado del Servicio de Inteligencia Alemán

Apreciado Sr. Uhrlau,
Tenemos diversos informes relacionados con el BN.
¿Podría ser más preciso?
Gracias.
Jay Lim.

Para: Sunshine Press Legal Office
Fecha: Jue, 19 Dic 2008 17:59:21
Asunto: Respuesta: Re: Informe clasificado del Servicio de Inteligencia Alemán.

Apreciado Sr. Lim.
A fecha de hoy ofrecen aún la posibilidad de descargar un informe clasificado del BND desde la dirección: http://www.wikileaks.com/wiki/BND_Kosovo_intelligence-report,_22_Feb_2005.
Le solicitamos una vez más que elimine ese archivo de inmediato, así como cualquier otro archivo o informe relacionado con el BND.
De lo contrario procederemos a demandarlos.

Atentamente, Ernst Uhrlau

Director del Servicio de Inteligencia Alemán."[308]

II.2.5.2. En las grandes filtraciones. En Asesinato Colateral se corroboró la información con el envío a Irak de los periodistas islandeses Kristinn Hrafnsson e Ingi Ragnar Ingasson, quienes hablaron con testigos oculares e investigaron el lugar donde se produjeron los hechos[309]. Determinante fue la ayuda del Ministerio de asuntos exteriores de Islandia, que cooperó para que sus connacionales llegaran a Bagdad, arribando luego más específicamente al barrio Al Amin, la zona de la ciudad donde se había producido la matanza[310].

Para verificar la autenticidad de los Diarios de guerra, Bill Keller, el editor ejecutivo de *The New York Times*, envió a Eric Schmitt, su experimentado corresponsal de guerra cuyos conocimientos de historia militar resultaban útiles y que desde los países envueltos pudo informar que sí parecían auténticos.

Los alemanes del *Der Spiegel* también resultaron fundamentales a la hora de corroborar la información, pues tenían acceso a la investigación que realizaba el parlamento federal alemán a la guerra de Afganistán, que también incluía material militar secreto estadounidense.[311]

II.2.6. ¿Hubo criterios de edición en la publicación de información para prevenir daños en las personas?

En un principio el material filtrado exponía los nombres de individuos y otras informaciones que los medios de comunicación tradicionales por lo general editan antes de sus publicaciones. Esto desafió uno de los principios más importantes de *WikiLeaks,* que era el de publicar todos los documentos que les llegaran sin censura alguna. Según sus palabras, eso tenía un "uso

[308] Idem, p. 58 - 59.
[309] Idem, p. 141 y 146.
[310] O´HAGAN, op. cit., p. 204.
[311] LEIGH y Harding, op. cit., p. 129.

estratégico". Con cada filtración se intentaba "ampliar un poco más los límites de lo realizable". Querían crear controversia acerca de la distinción entre lo público y lo privado en relación a las actuaciones de personas con poder emanado de la soberanía popular. [312]

Con el devenir estas ideas fueron evolucionando para evitar que los implicados inocentes pudieran sufrir consecuencias negativas. Desde ahora tendrían que pensar aquellos aspectos que pudiesen provocar problemas, no sólo a ellos, sino también a las fuentes, a los informantes y a los inocentes. El mismo Assange explica un matiz en su principio de transparencia, haciendo mención de ello en su autobiografía no autorizada: "No hablo de la transparencia en su máximo extremo (…) hablo de justicia", subrayando la necesidad de una combinación entre justicia y tecnología[313].

En 2010 con el lanzamiento del video *Collateral Murder*, *WikiLeaks* rompió no sólo con su principio básico de publicar documentos en su formato original, sin editar, sino también con su segundo principio esencial, el de publicar los documentos por orden de recepción.[314] La discrepancia entre la versión más corta y la más larga, además del título provocativo han sido interpretados como signos adicionales de la agenda política de *WikiLeaks*. Al mismo tiempo, el video fue la primera liberación que recibió la entrada sustancial de periodistas como la del Islandés Kristinn Hrafnasson y la del camarógrafo Ingi Ragnar Ingason que no sólo trabajaron en la redacción, sino que incluso viajaron a Irak para corroborar los hechos.[315]

[312] DOMSCHEIT-BERG, op. cit. p. 53. El hecho es que *WikiLeaks* en sus primeros días no redactó ningún documento. Fue uno de sus principios básicos el liberar los documentos en su formato original, sin editar, tal como se estipula en la sección de Preguntas Frecuentes en la página *web*.
[313] O´HAGAN, op. cit., p.127.
[314] MAURER, op. cit., p. 19, referencia n° 127.
[315] Idem, p. 20, referencia n° 128.

Esto sentó las bases para un esfuerzo mucho más grande, en cooperación ya no sólo con dos periodistas del pequeño país de Islandia, sino en colaboración con los que muchos consideran los líderes mundiales en el sector de los medios de comunicación escritos.

Para la publicación de los diarios de guerra de Afganistán, se acordó que el día coincidiera con el de la publicación de la revista semanal alemana para que así pudiera mantener su edición habitual. Pero, pocos días antes de ello, ocurrió una grave descoordinación: el portavoz de *WikiLeaks* de ese entonces cuenta que días antes de la publicación se reunió con dos periodistas del semanario, transcurriendo la reunión perfectamente, hasta que estos le preguntaron cómo iba el proceso de minimización de daños, lo que dijeron formaba parte de un acuerdo irrenunciable con Assange. Pero de aquel acuerdo el vocero no tenía conocimiento, aunque dice compartir su fondo que no es más que "los nombres de los inocentes implicados debían eliminarse". Ello supuso una dificultad intempestiva, editar los diarios en un breve tiempo.[316]

De esta manera, en definitiva fueron los medios de comunicación los que decidieron el criterio decisivo para publicar. Se introdujo un proceso de redacción en el que de lo publicado nada pusiera en peligro a ninguna fuente vulnerable ni hacer peligrar operaciones especiales en activo. Nunca existió un "vertido masivo"[317].

[316] DOMSCHEIT-BERG, op. cit. p. 165.
[317] LEIGH y Harding, op. cit., p. 19 – 20.

Así, se retiraron 14.000 de los 90.000 documentos y se esperó hasta nueva orden. Se trataba de los "informes de amenazas", en los que se incluía una relación de los afganos que habían actuado como informantes del ejército estadounidense, como por ejemplo, avisos de atentados planificados o ubicación de depósitos de armas. En los otros 76.000 todavía se encontraron un centenar de nombres.[318]

Luego de la publicación se decidió qué hacer con los otros 14.000 documentos. Los técnicos de *WikiLeaks* realizaron rápidamente un ingenioso *software* que permitió ampliar el círculo de ayudantes a los "amigos de los amigos" en el proceso de pulido, por lo que cientos de voluntarios pudieron visualizar y ayudar simultáneamente teniendo acceso a un pequeño paquete de datos, por lo que no podían ver todo lo que estaba en juego. Pronto, el proceso de afinado acabó y esta última información fue publicada en el dominio de los documentos de Afganistán, en un archivo de 1,4 gb, eso sí, encriptado. [319]

Según *The Guardian*, Assange no se preocupaba mucho sobre el daño a los informantes: "Bueno, son informantes", habría dicho. "Así que, si los matan, ellos tienen lo que se merecen. Se lo merecen."[320] Declaraciones desmentidas por Assange en su autobiografía no autorizada[321].

[318] Mientras se hacía este trabajo, Assange también enviaba ordenes vía *chat*: "Hay que comprobar si en la base de datos de Afganistán hay información que afecte a informantes inocentes. Dichas informaciones se encuentran sobretodo en los *threat reports* (informes de amenazas). Hay bastante trabajo para eliminarlas. DOMSCHEIT-BERG, op. cit. p. 166-167.
[319] Ello como forma de evitar que alguien desmantelara *WikiLeaks* o intentara secuestrar a alguien del equipo para que no se publicaran más documentos. Finalmente los técnicos trabajaron en un sistema para que las contraseñas se publicaran automáticamente en caso de que pasara algo, conocido como el método del *dead man switch* (pedal de hombre muerto).DOMSCHEIT-BERG, op. cit. p. 173 a 176.
[320] MAURER, op. cit., p. 20, referencia 130.
[321] O´HAGAN, op. cit., p. 240.

El periódico inglés de todas formas hace el siguiente reconocimiento: "Para ser justos con Assange, con el tiempo revisó su punto de vista [...] cinco meses después, Assange había abrazado completamente la lógica de la edición, con un papel casi como el de una editorial tradicional."[322] En retrospectiva, se podría argumentar que Assange parece haber pasado de ser un anarquista radical en el año 2006 a percibirse a sí mismo como un periodista o un editor en 2010.[323]

El personal de *WikiLeaks* habría emulado las ediciones de los medios de comunicación establecidos, lo que Assange llamó "la política de minimización de daño" de *WikiLeaks*. En este punto, *The Guardian* informa que *WikiLeaks* había adoptado todas sus redacciones.

Pero el profesor Maurer plantea que en *the Afghanistan War Diaries*, *WikiLeaks* todavía incluye los nombres de los individuos en los documentos accesibles en su sitio *web*, mientras que los tres principales medios de comunicación los editaron.[324] Lo mismo un poco matizadamente asegura el ex portavoz de *WikiLeaks*, Daniel Domscheit-Berg, diciendo que la edición lamentablemente no habría dado siempre los resultados deseados por *WikiLeaks* y sus colaboradores, como se demostró, según él, en la filtración sobre Afganistán.[325]-[326]

---

[322] MAURER, op. cit., p. 20, referencia 131.
[323] Idem, p. 21, referencia 140.
[324] Idem, p. 20, referencia 129.
[325] DOMSCHEIT-BERG, op. cit. p. 157.
[326] "(…) cinco ONG han instado por carta a *Wikileaks* a borrar los nombres de los afganos que colaboran con las fuerzas internacionales y pueden ser víctimas de represalias. Representantes de los talibanes han declarado públicamente que están chequeando los documentos y planean vengarse de quienes hayan colaborado con las fuerzas internacionales.
"Estamos muy preocupados por los riesgos y las posibles represalias contra los afganos cuyos nombres aparecen en los documentos de *Wikileaks*", declaró ayer a *France Presse* Nader Nadery, presidente de la Comisión Independiente para los Derechos Humanos en Afganistán (AIHRC, en sus siglas en inglés), una de las cinco ONG que firman la carta. Las otras son la Campaña por las Víctimas Inocentes de los Conflictos, el *International Crisis Group*, el *Open Society Institute* y Amnistía Internacional." El País, "Cinco ONG exigen a *WikiLeaks* que elimine los datos de los colaboradores afganos"**.** 11 de agosto de

Grupos de derechos humanos en Afganistán, así como organizaciones sin fines de lucro como Reporteros sin Fronteras, manifestaron su preocupación por la publicación de archivos militares de Estados Unidos en Afganistán[327]. Aparecían nombres de personas en el primer lote de archivos publicados que pudieron haber ocasionado riesgo[328]. El Secretario general de Reporteros sin Fronteras dijo que las acciones de *WikiLeaks* mostraron una "increíble irresponsabilidad" en la publicación de documentos militares estadounidenses clasificados sin editar.[329] El Pentágono acusó que los documentos publicados "dan a conocer los nombres de los afganos que colaboran con los militares de EE.UU."[330] Defendiendo sus acciones, Assange respondió: "Creemos que el camino hacia la justicia es la transparencia, y tenemos claro que el objetivo final es exponer las injusticias en el mundo y tratar de corregirlas"[331]

Pero en otra acción editorial, Assange, antes de la publicación, envió una petición al gobierno norteamericano a través de *The New York Times* solicitando información acerca del estándar en que una publicación podría constituir una amenaza para las personas.[332]

2010. [en línea] <http://elpais.com/diario/2010/08/11/internacional/1281477603_850215.html> [Consulta: 9/04/2013]

[327] BARRON, Jerome A., *"The Pentagon Papers case and the WikiLeaks controversy: National Securiry and the First Amendment"*. [El caso Papeles del Pentágono y la controversia WikiLeaks: Seguridad Nacional y la Primera Enmienda]. Wake Forest Journal of Law & Policy, Vol 1:1 2011, p. 63, referencia n° 112.

[328] Idem, referencia 113.

[329] Idem, referencia 114.

[330] Idem, referencia 115.

[331] Idem, referencia 116.

[332] DOMSCHEIT-BERG, op. cit., p. 229.

El contactarse con la autoridad constituía una práctica del *New York Times,* que junto con *Der Spiegel* se acercaron a la Casa Blanca antes de la publicación. Es más, incluso, *The New York Times* dio otra vez una alerta temprana a la Casa Blanca para la publicación de los cables el 19 de noviembre de 2010, proporcionando los 100 o 150 cables utilizados.[333]

Luego, *The Times*, rival de *The Guardian,* insinuó que los materiales filtrados causaron la muerte de un desertor talibán, lo que se habría comprobado falso, pues esta persona habría sido asesinada dos años antes.[334]

Mas tarde, para la publicación de los telegramas norteamericanos, se contó con muy poco tiempo y cierto apresuramiento. *The Guardian* quería publicar sin el consentimiento de Assange, pues como vimos además de no necesitarlo temía que la competencia se le adelantara. “El núcleo antiguo de *WikiLeaks* no habría aceptado jamás la publicación de los documentos en esos momentos” opinó Domscheit-Berg, aunque también coincide en que publicarlos es en sí misma una decisión correcta, difiriendo al parecer, otra vez, en que le hubiera gustado que se otorgara un mayor nivel de seguridad a los implicados[335] .

Los editores aseguraron de que se tuvo recaudo y que los cables se publicaron retocados. Se habría seleccionado la información de telegramas individuales si estos podían poner en peligro a una persona. Los periódicos explicaron que aquello se había acordado como condición recíproca irrenunciable. Por ejemplo, dicen haber acordado no publicar los nombres de los disidentes chinos, de periodistas rusos u opositores iraníes que habían hablado con los diplomáticos norteamericanos[336].

[333] MAURER, op. cit., p. 19, referencia 125.
[334] O´HAGAN, op. cit., p.230.
[335] DOMSCHEIT-BERG, op. cit., p. 236.
[336] Idem, p. 228-229.

Se defienden diciendo que cada periodista era responsable de editar sus propios cables eliminando cualquier fuente que pudiese correr algún riesgo de ser publicado su nombre. “Como norma, jefes de Estado, políticos muy conocidos, personas presentes en la vida pública en general, eran blancos legítimos. En algunas partes del mundo, sin embargo – Oriente Próximo, Rusia y Asia Central, Irak, Afganistán y Pakistán – incluso ser visto hablando con los estadounidenses era arriesgado”[337].

Nuevamente Assange intentó contactarse con las autoridades norteamericanas, envió una solicitud a la embajada estadounidense en Londres para hablar con el departamento de Estado. Oferta que fue rechazada[338]. La nota del 26 de Noviembre decía así:

“Desde *WikiLeaks*, les estaríamos muy agradecidos si el gobierno de los Estados Unidos pudiera indicarnos en qué casos no se puede descartar que la publicación de determinado telegrama puede suponer una amenaza para personas individuales”[339].

Prometía que *WikiLeaks* tomaría rápidamente cualquier propuesta del gobierno de Estados Unidos.

El consejero legal del Departamento de Estado le contestó tajantemente que los cables:

“se ofrecían violando las leyes de los Estados Unidos y sin ninguna consideración a las graves consecuencias de ese acto”.

El 28 volvió a escribir a la embajada de que no tenían la intención de poner en peligro a nadie ni:

[337] LEIGH y Harding, op. cit., p. 205.
[338] Idem, p. 22.
[339] DOMSCHEIT-BERG, op. cit., p. 229.

"(…) tampoco queremos dañar la seguridad nacional de Estados Unidos (…) Han decidido responder de una manera que me lleva a concluir que los riesgos son totalmente imaginarios y que, en cambio, lo único que les preocupa es suprimir las pruebas de abusos contra los derechos humanos y otras conductas criminales." [340]

Otro importante punto de su defensa, es que dicen haber publicado sólo 2 mil de los 250 mil cables diplomáticos, que "seis meses después de la primera publicación de los diarios de guerra, nadie ha sido capaz de demostrar que haya habido ningún perjuicio a vida o muerte"[341], y que incluso el 17 de Octubre de 2010, *CNN* informó que según un alto oficial de la OTAN en Kabul "no hubo ni un solo caso de afganos que necesitaran protección o traslado debido a la filtración"[342]-[343]

Finalmente, dicen los periodistas de *The Guardian*: "sería buena idea que alguien financiara algún estudio riguroso de alguna institución académica seria sobre el equilibrio resultante entre daños y beneficios", evaluar las ventajas e inconvenientes de la transparencia en lugar de provocar un salto instintivo hacia más secretismo[344].

[340] LEIGH y Harding, op. cit., p. 214 y 215.
[341] Idem, p. 20.
[342] Idem, p. 132.
[343] Puede llegar a ser de relevancia el leer una declaración de Assange sobre el punto: "Los que no entienden nuestro trabajo, los que no quieren entenderlo, se precipitan a afirmar que con él podríamos poner algunas vidas en peligro. Cuando en realidad lo que nos impulsa es fundamentalmente la idea de salvar vidas. Contribuyendo, en pro del interés de los pueblos, a que las guerras terminen, proporcionando a los periodistas los medios que les permitan controlar los excesos de poder, pretendemos limitar la sed de matanzas, los deseos de lanzar escaramuzas e invasiones, y también contrarrestar las mentiras con que esas operaciones suelen defenderse ante la luz pública". O´HAGAN, op. cit., p.210.
[344] LEIGH y Harding, op. cit., p. 23.

Meses después de la filtración de los cables, se informa, en Septiembre de 2011, que *WikiLeaks* "ha anunciado la publicación de la totalidad de los 251.287 cables diplomáticos a su disposición sin ocultar la identidad de las fuentes, según comunicó a sus seguidores a través de su cuenta de *Twitter*"[345]. Además, se informa que los cinco periódicos y Reporteros sin fronteras, le quitan temporalmente el apoyo a la organización.

WikiLeaks explica en su comunicado, que ha decidido hacerlo una vez que la clave que permitía acceder a los documentos encriptados había sido divulgada. La organización culpa al periódico *The Guardian* de exponer la clave en un libro publicado en febrero pasado sobre la organización de Assange. El diario ha rechazado cualquier tipo de responsabilidad en relación con la publicación de los cables íntegros. "*WikiLeaks* debe responsabilizarse de sus acciones en lugar de tratar de culpar a otros", ha indicado el diario británico en un comunicado. David Leigh, el periodista de *The Guardian* autor del libro titulado "*WikiLeaks* y Assange…", ha manifestado que fue Assange quien le aseguró que la clave funcionaría durante un breve periodo de tiempo y que por lo tanto ya no lo haría al tiempo de publicado el libro.[346]

[345] EL PAÍS, *"WikiLeaks anuncia la publicación de todos sus cables sin ocultar sus fuentes"*, 3 de septiembre de 2011, [en línea] <http://elpais.com/diario/2011/09/03/internacional/1315000809_850215.html> [Consulta: 08/07/2013]
[346] Idem.

*Der Spiege*l sostuvo que la publicación de los cables sin editar obedece a una "cadena de errores, descuidos, indiscreciones y confusiones" que perjudican la credibilidad de la organización de filtraciones y que podrían desanimar a futuras fuentes. Explica, por ejemplo, que voluntarios de *WikiLeaks* publicaron por equivocación una versión comprimida de la base de datos que contenía los cables diplomáticos. *Open Leak*, la *web* de Daniel Domscheit-Berg, el archirrival de Assange y antiguo portavoz de *WikiLeaks*, divulgó también la vía para acceder a la información confidencial procedente de las embajadas, con la supuesta intención de desprestigiar a *WikiLeaks*.[347]

La versión de Assange es que "La información ya estaba en la red. Las agencias de inteligencia y los gobiernos que necesitan ser reformados ya podían acceder al material. Era importante que la prensa pudiera tener la versión original. Nuestra obligación es maximizar las reformas y minimizar daños". Agrega que Domscheit - Berg sabía cómo llegar a la base de datos y su contraseña, que lo habría hecho para demostrar que *WikiLeaks* es una plataforma poco segura y que este pasó información a un periodista del semanario *Der Freitag* y, que a mediados de agosto *WikiLeaks* detectó que esa información empezaba a circular con fuerza en Internet.

[347] Idem.

Por su parte la versión de *The Guardian* es que "Assange nos aseguró que la contraseña estaría muerta una vez nos descargáramos los *papeles",* que el editor australiano no eliminó los archivos del servidor, como se suele hacer en estos casos, que en un descuido imperdonable, volvió a usar la misma contraseña para encriptar los mismos archivos*,* y que el origen de este enredo se encuentra a mediados de agosto, cuando Daniel Domscheit-Berg es expulsado del *Chaos Computer Club.* Algunos miembros del club lo acusaron de no devolver el material que se llevó de *WikiLeaks* cuando abandonó la organización. "Entonces, Domscheit-Berg decide vengarse", explica Leigh, periodista del medio inglés.[348]

Domscheit-Berg se defiende negando intenciones de vengarse. Coincide con Leigh en que probablemente fue Assange el que diseminó pistas por la Internet, que pasó información al periodista alemán para que pudiera comprobar que *WikiLeaks* no es un sitio seguro porque "estaba gravemente preocupado con la seguridad de *WikiLeaks* y su capacidad para controlar los datos", y que ese es el motivo por el cual aún no ha devuelto parte de la información que se llevó.[349]

II.3. ¿CUÁLES HAN SIDO LAS REACCIONES DE HECHO DE LA AUTORIDAD POLÍTICA?

[348] Idem.
[349] Idem.

En el contexto de la filtración de los cables diplomáticos, la primera reacción fue la del Presidente de los Estados Unidos, Barack Obama, quien habló con algunos jefes de Estado. Este tipo de control de daños, sin embargo, se llevó a cabo principalmente por el Departamento de Estado, mientras que el Departamento de Defensa volvió a examinar sus normas de seguridad cibernética.[350]

Pero la respuesta global de la autoridad política en sí misma, es mucho más compleja, y puede ser categorizada, para integrarla por los dos siguientes componentes principales: el material y el jurídico, comprendiéndose dentro del primero la respuesta física, tecnológica y mediática.

II.3.1. ¿Cuál ha sido su reacción material?

II.3.1.1. Respuesta Física. Aunque no es una posición oficial, existe un número de personas que pública y directamente pidió una respuesta física. El funcionario de más alta jerarquía del gobierno de los EE.UU. que se pronunció en este contexto, aunque indirectamente, fue el vicepresidente Biden, quien declaró que Assange es "más bien un terrorista de alta tecnología que un Papeles del Pentágono"[351].

Sarah Palin la ex gobernadora de Alaska, fue bastante más directa, denunció el "espionaje repugnante y antinorteamericano (…) ¿Por qué no se le ha perseguido con el mismo apremio con que perseguimos a *al-Qaeda* y los cabecillas talibanes? (…) Es un agente antinorteamericano, con sangre en las manos"[352].

[350] MAURER, op. cit., p. 27, referencia 191.
[351] Idem, p. 32, referencia 241.
[352] LEIGH y Harding, op. cit., p. 226

De la misma manera el congresista Peter T. King escribió una carta a Hillary Clinton, en la que afirmaba que Assange era jefe de una organización terrorista y que merecía ser tratado como tal.[353]

Más explícito aun fue Pete Hoekstra, un congresista de Michigan que ha sugerido la pena de muerte: "Está claro que podemos perseguir a la persona que filtró la información o *hackeó* nuestro sistema y que probablemente podemos hacerlo por espionaje y quizá traición. Si le damos caza y logramos condenarla por traición, entonces entra en juego la pena de muerte.[354]

Mike Rogers, su colega también de Michigan se expresa en la misma línea: "Defiendo que se considere la pena de muerte en este caso. Está claro que él ayudó al enemigo en lo que puede resultar la muerte de soldados estadounidenses o de los que colaboran con ellos. Si eso no es un delito capital, no sé qué es."[355]

Los periodistas del *The Guardian* hacen el contraste entre las débiles críticas que hubo a las filtraciones en el Reino Unido y lo asombroso que fue leer que personajes estadounidenses razonablemente populares llamaran a asesinar al líder de *WikiLeaks*.[356]

[353] O´HAGAN, op. cit., p. 20.
[354] LEIGH y Harding, op. cit., p. 225.
[355] Idem.
[356] Idem, p. 25.

II.3.1.2. Respuesta Tecnológica. La primera, más que respuesta, reacción tecnológica, fue la del Departamento de Defensa, que creó un "Grupo de Trabajo de Revisión de Información" que consta de 120 personas dirigidas por el general Robert A. Carr de la Agencia de Inteligencia de Defensa, con el objetivo de no sólo revisar los cables diplomáticos filtrados en el *Cablegate*, sino también para encontrar evidencia en contra de fuentes, de Assange y de *WikiLeaks.*[357]

En relación a si el gobierno de EE.UU. ha participado o no en un ataque cibernético contra *WikiLeaks,* no se tiene certeza.

La única evidencia de la participación del gobierno se reduce al senador Lieberman, presidente del Comité de Seguridad Nacional haciendo un llamado a que cualquier compañía u organización que aloje a *Wikileaks* termine inmediatamente su relación con ellos. Buscando instar a *Amazon* dijo que: "Los actos ilegales, escandalosos y temerarios de *WikiLeaks* han puesto en peligro nuestra seguridad nacional y en riesgo la vida de todo el mundo. Ninguna empresa responsable - ya sea estadounidense o extranjera - debe ayudar a *WikiLeaks* en sus esfuerzos por difundir estos materiales robados".[358]

[357] MAURER, op. cit., p. 32, referencia 237.
[358] LEIGH y Harding, op. cit., p. 226 y 228.

La secretaria Clinton declaró en su discurso del 15 de febrero de 2011 *Internet Rights and Wrongs: Choices & Challenges in a Networked World*: "Hubo informes en los días posteriores a estas fugas de que el gobierno de los Estados Unidos intervino para obligar a empresas privadas a negar el servicio a *WikiLeaks*. Ese no es el caso. Ahora, algunos políticos y expertos pidieron públicamente a las empresas desvincularse de *WikiLeaks*, mientras que otros los criticaron por ello. Los funcionarios públicos son parte de los debates públicos de nuestro país, pero hay una línea entre la expresión de opiniones y coaccionar conductas. Las decisiones comerciales que las empresas privadas puedan haber adoptado para cumplir sus propios valores o políticas respecto de *WikiLeaks* no se encuentran en la dirección de la administración Obama"[359].

Entonces, ¿qué pasó? El 29 de noviembre de 2010, después del lanzamiento del *Cablegate*, un Ataque Distribuído de Denegación de Servicio (*DDoS*) fue lanzado contra el sitio *web* de *WikiLeaks* por el *hacktivista "The Jester"*.[360] Alcanzando un máximo de 18Gbps, este ataque *DDoS* es ocho veces más grande que cualquier ataque *DDoS* anterior sobre *WikiLeaks*. Al parecer, alguien que controlaba un *botnet* (conjunto de robots informáticos) formado por decenas de miles de ordenadores *Windows* estaba coordinándolos en un intento de hacer que *wikileaks.org* se viniera abajo[361].

[359] MAURER, op. cit., p. 31, referencia 227.
[360] Idem, referencia 228.
[361] LEIGH y Harding, op. cit., p. 226 - 227.

Después de la declaración del senador Lieberman, la empresa *Amazon*, cuyo servidor estaba siendo utilizado por *WikiLeaks*, decidió poner fin a la relación comercial. *WikiLeaks* respondió con la publicación de su nueva *URL* a través de *Twitter* y cuando el gobierno de Francia tomó medidas con el nuevo servidor francés, un servidor en Suecia fue elegido finalmente, siendo el que disfrutó de una de las protecciones más fuertes a la libertad de expresión.[362] La nueva dirección *URL* devino *wikileaks.ch*, que si bien es un nombre de dominio *web* suizo, el sitio fue realmente entregado por el Partido Pirata sueco.

A los pocos días, 1.200 sitios espejo habían surgido a través de la Internet haciendo en gran parte ineficaces el ataque *DDoS* y las acciones de las empresas.[363] Sin embargo, las acciones de *PayPal* y de otros proveedores de servicios financieros (como *PostFinance, MasterCard* y *VisaEurope*[364]), limitaron exitosamente el acceso de *WikiLeaks* a los fondos existentes y a las nuevas donaciones mientras surgían preguntas importantes sobre la neutralidad de la red. Una nueva escalada en el ciber-conflicto podría haber tenido lugar si *WikiLeaks* hubiera decidido liberar la contraseña para descifrar el archivo "*insurance file*", un archivo altamente encriptado, publicado en Internet el 30 de julio de 2010, y enviado a una docena de personas en memorias USB que contiene todos los cables en formato sin editar.[365]

El senado alabó la "acertada decisión" de *Amazon* e instó a cualquier empresa que mantuviera vínculos con *WikiLeaks* a seguir el ejemplo trazado.[366]

[362] MAURER, op. cit., p. 31, referencia 231.
[363] Idem, referencia 232.
[364] LEIGH y Harding, op. cit., p. 229.
[365] MAURER, op. cit., p. 32, referencia 234.
[366] LEIGH y Harding, op. cit., p. 228.

El grupo *hacktivista Anonymous*, que se había hecho previamente conocido por sus actividades contra la Cienciología, decidió lanzar un contraataque. También dirigido a empresas como *Amazon, PayPal, MasterCard*, entre otros. Incluso llegaron a intervenir la cuenta de la tarjeta de crédito de Sarah Palin y atacaron la página de *PostFinance*. Esto era algo nuevo, algo así como un equivalente a una ruidosa manifestación política contra los intentos de restringir la información.[367]

II.3.1.3. Respuesta mediática. A diferencia de la eventual respuesta tecnológica del gobierno de Estados Unidos contra *WikiLeaks* después del lanzamiento de los cables, la respuesta mediática de la administración política estadounidense comenzó antes y podemos distinguirlas según la filtración de que se trate.

Con la fuga sobre Afganistán no se produjo una respuesta pública del Gobierno de Obama. Algunos sostienen que esto se debe a que la liberación en gran parte trataba de la estrategia de guerra de la administración predecesora.[368]

El 28 de julio de 2010, tres días después de la publicación sobre Afganistán, el general de división Campbell, uno de los comandantes de las fuerzas armadas estadounidenses en aquel país, dijo que: “cualquier clase de filtración de material clasificado que pueda producirse en cualquier momento puede en potencia causar daños a los militares que trabajan aquí cotidianamente”. Aunque reconoció que no había leído los documentos filtrados.[369]

[367] Idem, p. 230 - 231.
[368] MAURER, op. cit., p. 32, referencia 236.
[369] O´HAGAN, op. cit., p. 235.

Al día siguiente, en una rueda de prensa en el Pentágono, el secretario de defensa Gates y el almirante Mullen dieron a entender sus apreciaciones, declarando este último: “Diga lo que diga el Sr. Assange acerca del bien superior que él y su fuente pueden estar persiguiendo, la verdad es que a estas horas sus manos podrían estar ya manchadas de la sangre de algún joven soldado o de la de una familia afgana”[370]. (La misma expresión fue ocupada por la gobernadora Sarah Palin[371]).

De inmediato un periodista presente le preguntó: “(…) ¿tiene usted información sobre las personas que podrían haber muerto debido a la publicación de estas informaciones?”.

A lo que Mullen contestó: “Todavía…lo que me preocupa más de todo este asunto es que pienso que hay ciertos individuos no directamente implicados en esta clase de combates, y que revelan estas informaciones, que no deberían… desde mi punto de vista…que no están capacitados para valorar por qué razón esta clase de informaciones son introducidas rutinariamente en los canales clasificados que utilizamos de manera específica…Y si no se entiende estos y no se sabe esto, resulta muy difícil comprender el impacto, y específicamente el potencial que todo…que tiene todo esto a la hora de arriesgar las vidas de nuestra infantería y de nuestros marines, y de nuestras fuerzas aéreas, las de los militares pertenecientes a la coalición, así como…así como las de los ciudadanos afganos. Y no me cabe la menor duda al respecto”.

El secretario de defensa Gates intervino diciendo a continuación: “Me gustaría añadir…Quiero añadir una cosa más. Lo que no debemos olvidar es que se trata de una enorme cantidad de datos no elaborados…No hay responsabilidad. No hay ningún sentido de la responsabilidad. Por así decirlo, lanzan todo eso por ahí, y al diablo con las consecuencias.”

[370] Idem.
[371] Idem, p. 22.

Ante estas declaraciones el periodista dijo finalmente: “Con el debido respeto, no han respondido ustedes a mi pregunta.”[372]

Siguiendo la misma línea, según el ex portavoz de *WikiLeaks*, hasta la fecha “ni un solo informante ha sido perjudicado debido a la publicación de aquellos informes”.[373] Y agrega: “Más tarde se ha sabido que el Ministerio de Defensa estadounidense no tardó en clasificar la información como inofensiva en un comunicado interno”.[374]

La misma información agrega Assange: “Forzado a decir la verdad, en una carta dirigida al Senado dos semanas después, el 16 de agosto de 2010, el secretario de defensa, Gates, informó a los miembros de esa cámara que “los análisis realizados hasta la fecha no han demostrado que, debido a estas revelaciones, hayan corrido riesgo alguno ni las fuentes de inteligencia ni los métodos empleados por ellas”[375].

También en esos meses ya se comienzan a expresar ciertas distinciones dentro de la estrategia comunicacional y futura estrategia legal de Estados Unidos.

[372] Idem, p. 235 - 236.
[373] DOMSCHEIT-BERG, op. cit. p. 169.
[374] Idem.
[375] O´HAGAN, op. cit., p. 238.

En agosto de 2010, George Morell, secretario de prensa declaró: “Si a ellos no les parece que tener un buen comportamiento es una motivación suficiente, seremos nosotros los que tendremos que pensar de qué alternativas disponemos para forzarles a comportarse bien. Y permítanme que no añada más”. Cuando se le pregunto instante seguido si *The New York Times* como socio de *WikiLeaks* sería forzado también a comportarse, respondió: “Me parece que *The New York Times* no se considera a sí mismo como socio de ellos…Me parece que ni *The New York Times* ni el resto de las publicaciones están en posesión de estos documentos”. Entonces, ya se percibe que, a diferencia de sus asociados, se buscaría que *WikiLeaks* no recibiera trato de editor, sino que de espía.[376]

En la siguiente publicación, la liberación de los diarios de Irak, la respuesta fue en conjunto: EE.UU., Reino Unido y sus aliados reaccionaron ante las filtraciones justificando este tremendo derramamiento de sangre diciendo que de cualquier manera habían rescatado a los iraquíes de la brutalidad de Saddam Hussein.[377]

Finalmente, la respuesta mediática del gobierno estadounidense al *Cablegate* - que incluyó muchos cables de la administración Obama y no sólo se limitó temporalmente a la de Bush hijo - se volvió, naturalmente, más agresiva.

En noviembre de 2010 la secretaria de Estado, Hillary Clinton, declaró que la liberación no es "sólo un ataque a los intereses de política exterior de los Estados Unidos. Es un ataque a la comunidad internacional”.[378]

---

[376] Idem, p. 246.
[377] LEIGH y Harding, op. cit., p.150.
[378] EL PAIS, “Clinton tacha la filtración de “robo” y ataque a la comunidad internacional”, [en línea] <http://elpais.com/diario/2010/11/30/internacional/1291071608_850215.html> [Consulta 12/12/2012]

Lo contradictorio es que, en Enero del mismo año, en un discurso bastante innovador se expresó acerca de lo que llamó “un nuevo sistema nervioso para nuestro planeta”. Describió su visión acerca de las publicaciones digitales semiclandestinas, las llamó “el *samizdat* de nuestros días”[379], bandera de la transparencia y retador del viejo orden mundial autocrático y corrupto, advirtiendo que los gobiernos represivos “cargarían contra los pensadores independientes que utilizan estas herramientas”[380]. En el mismo discurso también dijo que “En muchos aspectos, la información nunca ha sido tan libre. (…) Incluso en los países autoritarios, las redes de información están ayudando a la gente a descubrir nuevos hechos y hacer que los gobiernos sean más responsables".[381]

Luego de las críticas a estas contradicciones, el 15 de febrero de 2011 Clinton respondió, reafirmando lo que para ella es el compromiso de la administración Obama con una Internet libre, declarando que "El hecho de que *WikiLeaks* utilice la Internet no es la razón por la que criticamos su actuar. *Wikileaks* no desafía nuestro compromiso con la libertad en Internet."[382]

Según *Der Spiegel*, el gobierno norteamericano argumentó de dos maneras: En primer lugar, que los cables no revelan nada nuevo, como lo declara el Presidente en su discurso en el Jardín de las Rosas, pero en segundo lugar, que la información pone en riesgo las vidas de las personas.[383] *The New York Times* añade un tercer argumento del gobierno, el de que al trabajar con *WikiLeaks*, las organizaciones de noticias "comprometen su imparcialidad e independencia."[384]

---

[379] Copia y distribución clandestina de la literatura prohibida por el régimen soviético y, por extensión, también por los gobiernos comunistas del bloque del Este durante la guerra fría.
[380] LEIGH y Harding, op. cit., p. 16.
[381] MAURER, op. cit., p. 33, referencia 250. Enero de 2010, en el *Newseum* en Washington.
[382] Idem, referencia 251.
[383] Idem, referencia 243.
[384] Idem, referencia 244.

Con respecto a la reacción del gobierno de Estados Unidos con los medios de comunicación, la Casa Blanca envió un correo electrónico a organizaciones de medios afirmando que *WikiLeaks* no es objetiva, sino que está contra EE.UU.[385] Solicitó retener la información para proteger, primero, a los informantes; segundo, a programas sensibles para los EE.UU.; y tercero, a los esfuerzos antiterroristas. Aparte de eso, el gobierno norteamericano se enfocó en que Manning ya había sido detenido y en *WikiLeaks*.[386]

Sin embargo, la Casa Blanca agregó más adelante una cuarta solicitud, que cualquier información relacionada con el interés nacional, así como los nombres de los dignatarios extranjeros debían ser retenidos.[387]

The New York Times expresó haber estado casi completamente de acuerdo con lo primero, que retendrá algo de información respecto a lo segundo y tercero, y que respecto al cuarto punto añadido últimamente estaban mayormente poco convencidos.[388]

[385] MAURER, op. cit., p. 33, referencia 246.
[386] Idem, referencia 247.
[387] Idem, referencia 248.
[388] Idem, referencia 249.

CAPÍTULO III

¿CUÁL HA SIDO LA REACCIÓN JURÍDICA DE LA AUTORIDAD POLÍTICA? ¿QUÉ DECISIONES HA TOMADO LA JURISPRUDENCIA ESTADOUNIDENSE? ¿QUE PREGUNTAS SE HA HECHO LA DOCTRINA?

III.1. ¿CUÁL HA SIDO LA REACCIÓN JURÍDICA DE LA AUTORIDAD POLÍTICA?

Existen importantes hechos públicos que hacen llegar a la razonable convicción de que Estados Unidos busca llevar a Assange a sus tribunales.[389]

[389] Ya hicimos mención anteriormente a las reacciones de importantes funcionarios del gobierno norteamericano. Recapitulemos:
1.- El vicepresidente Biden, quien declaró que Assange es "más bien un terrorista de alta tecnología que un Papeles del Pentágono".
2.- Sarah Palin, ex gobernadora de Alaska, dijo que se trataba de un "espionaje repugnante y antinorteamericano (…) ¿Por qué no se le ha perseguido con el mismo apremio con que perseguimos a *al-Qaeda* y los cabecillas talibanes? (…) Es un agente antinorteamericano, con sangre en las manos".
3.- El congresista Peter T. King escribió una carta a Hillary Clinton, en la que afirmaba que Assange era jefe de una organización terrorista y que merecía ser tratado como tal.
4.- Otro congresista, esta vez de Michigan, Pete Hoekstra, sugirió la pena de muerte: "Está claro que podemos perseguir a la persona que filtró la información o *hackeó* nuestro sistema y que probablemente podemos hacerlo por espionaje y quizá traición. Si le damos caza y logramos condenarla por traición, entonces entra en juego la pena de muerte".
5.- Mike Rogers, su colega también de Michigan dijo: "Defiendo que se considere la pena de muerte en este caso. Está claro que él ayudó al enemigo en lo que puede resultar la muerte de soldados estadounidenses o de los que colaboran con ellos. Si eso no es un delito capital, no sé qué es."

Desde los dichos de estos representantes del pueblo norteamericano surgen las siguientes dudas, que serán resueltas durante el transcurso de esta tesis: ¿Los actos de *WikiLeaks* son ciberterroristas? ¿Los actos de *WikiLeaks* constituyen espionaje? ¿Entra en juego la pena de muerte?

Para hacerlo más explícito, el fiscal general del presidente Obama, Eric Holder, citó a conferencia de prensa para anunciar que había "en curso una investigación criminal activa" por la filtración de información clasificada, y prometiendo que se harían cargo de hacer valer las responsabilidades de quienes, según él, rompieran las leyes estadounidenses, dijo: "En la medida en que hay vacíos en nuestras leyes, actuaremos para llenarlos, lo cual no significa que, en estos momentos, haya alguien que, debido a su ciudadanía o residencia, no sea blanco o sujeto de una investigación que está en marcha". [390]

De todas formas, las posibilidades de que una respuesta legal surta efecto están limitadas por los problemas generales del derecho informático. Nos referimos a la incertidumbre jurisdiccional en una Internet teóricamente sin fronteras y el problema de la atribución[391], así como sus imprevistas consecuencias[392].

---

[390] LEIGH y Harding, op. cit., p. 232.

[391] "Un ejemplo de ellos se dio en el caso del banco *Jullius Bär*, una de las primeras "víctimas" de un comunicado de *WikiLeaks* al dejar expuesto su blanqueo de capitales. A *Bär* le resultó difícil determinar en qué país las fugas podrían ser consideradas ilegales y contra quién presentar cargos. El banco finalmente decidió actuar persiguiendo la responsabilidad de Daniel Mathews, cuyo nombre era uno de los pocos públicamente asociados con *WikiLeaks* al declararlo su página *web* y que, además, podría ser procesado en Estados Unidos porque estudiaba en Stanford. Sin embargo, Mathews fue apoyado entre otros por la Unión Americana de Libertades Civiles y la Fundación Frontera Electrónica. Finalmente el caso *Bär* cayó. MAURER, op. cit., p. 27, referencia 194.

Si bien durante el transcurso de nuestra investigación dilucidaremos la aplicabilidad de los distintas leyes estadounidenses que según la doctrina de ese país podrían ponerse en juego en la experiencia *WikiLeaks* y contra la persona de Julian Assange en el evento de tener que enfrentar a los tribunales norteamericanos, resulta también de interés la reflexión y el aporte del renombrado administrativista argentino residente en España, Beltrán Gambier, en relación a la situación jurídica que se vive hasta este momento, es decir, que Julian Assange se encuentra refugiado en la embajada de Ecuador en Londres requerido por la justicia inglesa por a su vez haber sido requerido por la justicia de Suecia ¿Cómo podemos salvar los problemas de jurisdicción pendientes? Plantea el jurista que "en primer término se otorgue un "salvoconducto condicionado" para que Assange pueda ser conducido a la embajada ecuatoriana en Suecia, con lo cual, se logra dar cumplimiento a la orden de la justicia británica, salvando así la posición de este país, y la de Ecuador, que ha concedido asilo y quiere proteger su decisión diplomática. Pero además, al entregarse a Suecia, este país también sale indemne puesto que sus fiscales interrogarán y sus jueces juzgarán, si cabe, a Assange. Esta singular modalidad de salvoconducto debe garantizar que el destino del retenido sea precisamente Suecia y que viajará bajo la protección ecuatoriana. Es decir, el Reino Unido logra que su aceptación de la euroorden se cumpla. Pero que se cumpla de manera que, al mismo tiempo, permita garantizar el asilo concedido por Ecuador, no de cualquier manera.

De esta manera, el gobierno de EE.UU. adoptó acciones para estructurar un frente legal. Primero, los grupos de trabajo de los Departamentos de Defensa y de Estado no se establecieron sólo para manejar las liberaciones, sino que también para investigar criminalmente,[393] lo que condujo a la detención de Manning. El Ejército sin embargo, sólo tiene competencia sobre los miembros de su servicio. La investigación contra Assange y *WikiLeaks* es de la competencia del Departamento de Justicia.[394]

Contemporánea a estos sucesos, el gobierno sueco emitió una orden de arresto contra Assange acusándolo de agresión sexual.[395]. El líder de *WikiLeaks* pasó a la clandestinidad y los suecos entregaron el asunto a

---

En segundo lugar el punto de destino es otra embajada ecuatoriana, pero en Suecia. Así este país, logra que sea su jurisdicción la juzgadora, de conformidad con la entrega británica en cumplimiento de la euroorden. Esto requerirá cierta flexibilidad procesal por parte de Suecia dada la particular condición de Assange, pero de ninguna manera un debilitamiento de su potestad jurisdiccional. Pero es necesario que quede claro que el sometimiento de Assange es solo a los tribunales suecos, sin que en modo alguno pueda ser extraditado a Estados Unidos, puesto que además de su compromiso, gozaría de la protección diplomática de Ecuador ante Estados Unidos.

Si la efectiva finalidad de la extradición a Suecia es la de que Assange sea juzgado por dos (o más) supuestos delitos (o faltas) sexuales entonces todo se cumple perfectamente en esta audaz y hábil "Solución Gambier". Solución que naturalmente, para lo que no está, es para otras cosas, como por ejemplo, para entregar a los Estados Unidos a un sujeto que le ha hecho una demostración de que su sistema informático militar no es perfecto y que las crueles barbaridades que se narraban en algunos documentos, resultan que han salido a la luz. Para eso, desde luego, no está la "Solución Gambier" ni ninguna otra. Para eso está solamente la terrible "raison d'État," que es, exactamente, lo que nos tememos -y debe temerse Assange- que esté detrás de todo, y que aplicada al caso, consiste literalmente en acabar con el "enemigo del Estado". EL IMPARCIAL, *"Caso Assange: La solución Gambier:"*, 3 de Octubre de 2012, [en línea] <http://www.elimparcial.es/mundo/caso-assange-la-solucion-gambier-112077.html> [Consulta: 25/11/2013].

[392] Una segunda restricción en la ciber-ley son las consecuencias imprevistas. Barbara Streisand experimentó en 2003 hoy se conoce como el "efecto Streisand". Mike Masnick de Techdirt acuñó este término para describir el "fenómeno de la Internet en el que un intento de ocultar o quitar una pieza de información tiene la consecuencia no deseada de dar a conocer la información más ampliamente".Domscheit-Berg revela que *WikiLeaks* incluye claramente estos efectos en su estrategia: "nosotros [...] tenemos la esperanza de que la Cienciología trate de demandarnos. La secta seguramente habría perdido cualquier demanda que optase por presentar, y el caso habría atraído más interés público a los documentos rimbombantes, como había sido con el caso *Julius Bär*". MAURER, op. cit., p. 28.

[393] MAURER, op. cit., p. 29, referencia 206.

[394] Idem, referencia 207.

[395] BARRON, op. cit., p. 66, referencia 133.

Interpol[396]. El acusado negó los cargos y dijo que eran "parte de un complot para silenciar a *WikiLeaks*"[397].

En diciembre de 2010 se entregó a autoridades británicas en Londres[398]. Después de considerar la solicitud de extradición del gobierno sueco, un juez británico concluyó que había riesgo de fuga, negando la libertad bajo fianza[399], concediéndosela más tarde[400]. En febrero de 2011, se aprobó la solicitud de extradición del gobierno sueco[401]. En noviembre Assange pierde la apelación[402]. En junio de 2012 la Corte Suprema de Inglaterra rechaza el recurso que buscó evitar su extradición a Suecia, por lo que sería entregado a autoridades de ese país el 7 de julio[403]. El 19 de junio Assange viola su libertad bajo fianza y se refugia en la embajada de Ecuador solicitando asilo[404]. El 15 de Agosto el canciller ecuatoriano denunció que el gobierno británico habría amenazado con entrar a la fuerza para arrestar a Assange. Finalmente, el 16 de Agosto se le otorga asilo, situación que permanece vigente[405].

Así las cosas Estados Unidos suma una nueva dificultad para meter en una cárcel suya a Assange, pues, por otra parte, aun cambiando radicalmente el curso de los acontecimientos, si Assange pierde su protección y es extraditado a Suecia lo más probable es que ese país lo juzgue primero y en el

[396] Idem, referencia 134.
[397] Idem, referencia 135.
[398] Idem, referencia 136.
[399] Idem, referencia 137
[400] Idem, referencia 138.
[401] Idem, referencia 139.
[402] EL PAIS, "*Un tribunal de Londres aprueba la extradición de Julian Assange a Suecia"*, 2 de noviembre de 2011; [en línea] <http://internacional.elpais.com/internacional/2011/11/02/actualidad/1320221857_945649.html> [Consulta: 08/07/2013].
[403] EL PAIS, *"La Corte Suprema británica rechaza el recurso de Julian Assange"*, 14 de junio de 2012, [en línea]<http://internacional.elpais.com/internacional/2012/06/14/actualidad/1339682033_882446.html> [Consulta: 08/07/2013].
[404][en línea] <http://es.wikipedia.org/wiki/Crisis_diplom%C3%A1tica_entre_Ecuador_y_Reino_Unido_de_2012-2013> [Consulta: 08/07/2013].
[405] Idem.

evento de condenarlo que sea en ese país donde sea encarcelado y acallado. ¿Pero Estados Unidos tendrá un auténtico interés en juzgarlo en sus tribunales? ¿Será la "hipótesis del castigo sueco" la ideal para Estados Unidos al no verse expuesto a tener que llevar a cabo acciones propias para silenciarlo, ni enfrentar los comentarios de los noticieros mundiales y sus opiniones públicas, ni verse con la obligación de sobrepasar la pesada carga de la Primera Enmienda en cuyo juicio probablemente se ventilarían aun más crímenes de guerra? ¿O será que una no muy lejana a la ideal sea la que se vive incluso hoy al encontrarnos todos los habitantes de la Tierra en conocimiento de que de tener en mente la realización de fugas de material que contenga información sobre masacres que el gobierno estadounidense quiera mantener en secreto seremos destinatarios de una persecución ilimitada y siempre latente? [406]. En el mediano plazo no tendremos respuestas a esas preguntas, tal vez nunca las tengamos, pero podemos llegar a certezas bastante razonables. Por lo pronto y para enfocarnos en la pregunta de tesis imaginemos que las autoridades estadounidenses no dejaron siquiera un día de luchar por obtener del que Ecuador dejara de proteger a Assange presionando fuerte y decididamente tanto en lo económico como en lo diplomático en defensa de los valores de la democracia del norte y que finalmente lo han conseguido, y que Suecia archivó su investigación. El gobierno de Estados Unidos respira tranquilo, han logrado llevar a Assange a su jurisdicción nacional.

III.2. LA LEY ESTADOUNIDENSE.

III.2.1. Tratados Multilaterales firmados por Estados Unidos.

[406] BARRON, op. cit., p. 67, referencia 143.

III.2.1.1. Convención Americana sobre Derechos Humanos. Firmada por Estados Unidos en 1977, no ha sido ratificada, por lo que no se le ha otorgado competencia ni a la Comisión ni a la Corte Interamericana siendo en definitiva inoponible a Estados Unidos sus preceptos debido al no otorgamiento de operatividad a las instituciones del Pacto. [407]

Sin embargo, de todas formas la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Catalina Botero Marino, junto al Relator Especial de las Naciones Unidas Para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, Frank LaRue, en diciembre de 2010 declararon lo siguiente[408]:

"Ante los acontecimientos relacionados con la divulgación de comunicaciones diplomáticas por parte de la organización *WikiLeaks* y la posterior publicación de dicha información en los medios masivos de comunicación (…) [los relatores] consideran oportuno poner de presente una serie de principios jurídicos internacionales. Los relatores hacen un llamado a los Estados y a los demás actores relevantes para que tengan en cuenta los mencionados principios al responder a los acontecimientos mencionados.

"1. El derecho de acceso a la información en poder de autoridades públicas es un derecho humano fundamental sometido a un estricto régimen de excepciones. El derecho a la libertad de expresión protege el derecho de toda persona a tener libre acceso a la información pública y a conocer las actuaciones de los gobiernos. Se trata de un derecho particularmente importante para la consolidación, el funcionamiento y la preservación de los sistemas democráticos, por lo cual ha recibido un alto grado de atención por parte de la comunidad internacional. Sin la garantía de este derecho sería imposible conocer la verdad, exigir una adecuada rendición de cuentas y ejercer de manera integral los derechos de participación política. Las autoridades nacionales deben adoptar medidas activas a fin de asegurar el principio de máxima transparencia, derrotar la cultura del secreto que todavía

[407] CONVENCION AMERICANA SOBRE DERECHOS HUMANOS, Artículos 45 y 62 [en línea] <http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm> [Consulta: 26/08/2013]. Para ver el estado actual de firmas y ratificaciones de la Convención <http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos_firmas.htm> > [Consulta: 26/08/2013].

[408] BOTERO y LA RUE, *"Declaración conjunta sobre WikiLeaks"*, [en línea] <http://www.oas.org/es/cidh/expresion/showarticle.as p?artID=829&lID=2> [Consulta: 26/08/2013].

prevalece en muchos países y aumentar el flujo de información sujeta a divulgación.

2. En todo caso, el derecho de acceso a la información debe estar sometido a un sistema limitado de excepciones, orientadas a proteger intereses públicos o privados preeminentes, como la seguridad nacional o los derechos y la seguridad de las personas. Las leyes que regulan el carácter secreto de la información deben definir con exactitud el concepto de seguridad nacional y especificar claramente los criterios que deben aplicarse para determinar si cierta información puede o no declararse secreta. Las excepciones al derecho de acceso a la información basadas, entre otras razones, en la seguridad nacional deberán aplicarse únicamente cuando exista un riesgo cierto de daño sustancial a los intereses protegidos y cuando ese daño sea superior al interés general del público de consultar dicha información. Resulta contrario a los estándares internacionales considerar información reservada o clasificada la referente a violaciones de derechos humanos.

3. Es responsabilidad exclusiva de las autoridades públicas y sus funcionarios mantener la confidencialidad de la información legítimamente reservada que se encuentre bajo su control. Las otras personas, como los periodistas, integrantes de medios de comunicación o miembros de la sociedad civil que tengan acceso y difundan información reservada por considerarla de interés público, no deben ser sometidas a sanciones por violación del deber de reserva, a menos que hubiesen cometido fraude u otro delito para obtenerla. Los denunciantes ("*whistleblowers*") que, siendo empleados gubernamentales, divulguen información sobre violaciones del ordenamiento jurídico, casos graves de corrupción, la existencia de una amenaza grave para la salud, la seguridad o el medio ambiente, o violaciones de derechos humanos o del derecho internacional humanitario deberán estar protegidos frente sanciones legales, administrativas o laborales siempre que hayan actuado de buena fe. Cualquier intento de imponer sanciones ulteriores contra quienes difunden información reservada debe fundamentarse en leyes previamente establecidas aplicadas por órganos imparciales e independientes con garantías plenas de debido proceso, incluyendo el derecho de recurrir el fallo.

4. La injerencia ilegítima o las presiones directas o indirectas de los gobiernos respecto de cualquier expresión o información difundida a través de cualquier medio de comunicación oral, escrito, artístico, visual o electrónico, para incidir en su contenido por razones políticas, deben estar prohibidas por la ley. Esta injerencia ilegítima incluye las acciones interpuestas por motivos políticos contra periodistas y medios de comunicación independientes, y el bloqueo de sitios web y dominios de

Internet por causas políticas. En particular, es inaceptable que los funcionarios públicos sugieran la comisión de actos ilegítimos de represalia contra quienes han difundido información reservada.

5. Los bloqueos o sistemas de filtración de Internet no controlados por usuarios finales, impuestos por un proveedor gubernamental o comercial del servicio son una forma de censura previa y no pueden ser justificados. Las empresas que proveen servicios de Internet deben esforzarse para asegurar que se respeten los derechos de sus clientes de usar Internet sin interferencias arbitrarias.

6. Los mecanismos periodísticos de autorregulación han contribuido significativamente a desarrollar buenas prácticas sobre cómo abordar y comunicar temas complejos y sensibles. La responsabilidad periodística es especialmente necesaria cuando se reporta información de fuentes confidenciales que puede afectar valiosos bienes jurídicamente protegidos como los derechos fundamentales o la seguridad de las personas. Los códigos de ética para periodistas deben contemplar la necesidad de evaluar el interés público en conocer la información. Dichos códigos también resultan de utilidad para las nuevas formas de comunicación y para los nuevos medios, los cuales deben adoptar voluntariamente buenas prácticas éticas para asegurar, entre otras cosas, que la información publicada sea precisa, presentada imparcialmente, y que no cause daño sustancial y desproporcionado a bienes jurídicos legítimamente protegidos por las leyes como los derechos humanos.

Primero que todo los observadores destacan que el derecho de los ciudadanos a acceder a la información en poder de sus representantes es un derecho humano fundamental y que sus excepciones se deben designar estrictamente, subrayando a su vez que el derecho a la libertad de expresión es particularmente importante para la consolidación y preservación de la democracia.

Dicen que las excepciones a estos derechos están vinculadas a la protección de la seguridad nacional y los derechos y la seguridad de las personas, debiéndose definir con precisión el concepto antedicho y especificarse claramente los criterios para decidir que una información se declara secreta, generándose excepciones al derecho a la información sólo cuando exista un riesgo cierto de daño sustancial a los intereses protegidos y

cuando ese daño sea superior al interés general del público a informarse, siendo de suma importancia destacar que según los observadores, es contrario a los estándares internacionales considerar información reservada o clasificada la referente a violaciones a los derechos humanos.

Nos aclaran que la confidencialidad de la información reservada es de responsabilidad exclusiva de las autoridades institucionales, y que las demás personas no deben ser sometidas a sanciones al difundirla, exceptuados los casos de fraude o comisión de delito para obtenerla. Cuando el denunciante es empleado público este debe ser protegido frente a sanciones legales salvo que hayan actuado de mala fe.

Declaran también, que las presiones de los gobiernos respecto de cualquier expresión deben estar prohibidas por la ley. De mucho interés también es que hayan declarado que los bloqueos o sistemas de filtración de Internet no controlados por usuarios finales, impuestos por un proveedor gubernamental o comercial son una forma de censura previa injustificable.

Finalmente manifiestan que los mecanismos periodísticos de autorregulación deben seguir estableciendo buenas prácticas éticas para asegurar información precisa, imparcial y que no cause daño sustancial y desproporcionado a bienes jurídicos legítimamente protegidos por las leyes como los derechos humanos.

III.2.2. La Primera Enmienda de la Constitución Estadounidense.

"El Congreso no legislará respecto al establecimiento de una religión o a la prohibición del libre ejercicio de la misma; ni impondrá obstáculos a la libertad de expresión o de la prensa; ni coartará el derecho del pueblo para reunirse pacíficamente y para pedir al gobierno la reparación de agravios"[409].

[409] PRIMERA ENMIENDA A LA CONSTITUCIÓN DE LOS ESTADOS UNIDOS DE NORTEAMERICA [en línea] <http://www.law.cornell.edu/constitution/first_amendment> [Consulta: 06/05/2013].

III.2.2.1. ¿Cómo se desenvuelve?

Los estudiosos que han reflexionado sobre el ejercicio de esta amplia libertad de expresión y de prensa que en principio protege todas las formas de expresión y de información, no sólo lo hacen acerca de los espacios físicos en que se desenvuelve, sino que también a propósito de los espacios virtuales de propiedad privada, como la televisión por cable (propiedad de empresas de telefonía y de cable) y de señales inalámbricas (empresas satelitales, telefónicas). Estos espacios virtuales son fundamentales para la libertad de expresión.[410]

La arquitectura del derecho constitucional estadounidense se estructura de dos maneras: a través de las decisiones judiciales y mediante decisiones legislativas permitidas por el poder judicial. Mientras que el papel de las decisiones judiciales en el derecho constitucional es ampliamente aceptado, la idea de que las decisiones legislativas generen derecho constitucional pueden suscitar un poco de resistencia, ya que el poder judicial es supremo en la enunciación de las normas constitucionales. La supremacía judicial es aun más fuerte a propósito de la libertad de expresión. [411]

III.2.2.1.a. Modelo estándar de la Primera Enmienda. Este modelo se basa en hipótesis descriptivas e interpretativas sobre los precedentes. El modelo estándar, como muchos modelos doctrinales, comienza con casos paradigmáticos. A partir de estos casos paradigmáticos se infieren principios subyacentes. A continuación, estos principios se consideran los principios "fundamentales" que subyacen en la doctrina de la Primera Enmienda. Luego, se podrá evaluar normativamente otros casos, para determinar si se ajustan a

[410] AMMORI, Marvin. "*First Amendment Architecture*". [Architectura de la Primera Enmienda]. Stanford Law School - Center for Internet & Society; New America Foundation - Open Technology Initiative, 11 de Marzo de 2011, Wisconsin Law Review, Vol. 2012, No. 1, 2012, p. 8 y 9.
[411] Idem, p. 10 y 11.

estos principios “básicos” de la Primera Enmienda. Al aplicar estos principios, los casos que no se ajusten a ellos son “excepcionales”.[412]

III.2.2.1.b. Principios de la Primera Enmienda. Según el profesor Ammori son cinco los que se generan a través de los precedentes y la práctica. Algunos explícitos, invocados en varias oportunidades en resoluciones, otros más implícitos:[413]

El primer principio es el de los Espacios suficientes; El segundo es el de los Espacios adicionales, designados o discrecionales; El tercero es el de las Fuentes diversas y antagónicas; El cuarto principio es el de los Espacios para la formación del discurso nacional y local; y el quinto es el del Acceso Universal.

III.2.2.1.b.1. Primer Principio: de los espacios suficientes. Debe existir una medida de espacios tanto para la autonomía, la expresión y las funciones democráticas básicas.[414]

Espacios para la Autonomía. Con el objetivo de asegurar espacios para la autonomía del individuo en democracia, el poder judicial establece un espacio de “respeto especial”[415], el hogar familiar. Una democracia debe respetar la autonomía individual, un espacio para la reflexión y el análisis asegurando que los individuos tienen una barrera entre el yo y la “esfera pública” o el gobierno.[416]-[417]

---

[412] Idem, p. 12 y 13.
[413] Idem, p. 24.
[414] Idem, p. 28.
[415] Idem, p. 29, referencia 162, citando a su vez *City of Ladue v. Gilleo*, 512 U.S. 43, 57-58 (1994). *Cf.* John Fee, *Eminent Domain and the Sanctity of Home*, 81 NOTRE DAME L. REV. 783, 786–88 (2006); Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 Cornell L. Rev. 905, 913 (2010).
[416] Idem, p. 29.
[417] En *Stanley vs. Georgia*, la Corte sostuvo que el Estado no puede prohibir la posesión de material obsceno que se encuentre en la casa de alguien, aunque las expresiones “obscenas” no reciban protección en otros espacios. Idem, referencia 168, citando a su vez *Roth vs. United States*, 354 U.S. 476 (1957). El Tribunal de Justicia declaró que un Estado “no tiene por qué decirle a un hombre, sentado solo en su casa,

En consecuencia se pueden silenciar otras expresiones. La Corte ha confirmado las leyes que limitan los correos ofensivos[418], las emisiones de radio ofensivas[419] y los *sound trucks* ofensivos[420], subrayando, eso sí, que en espacios comunicativos públicos el gobierno no puede proteger a los oyentes del discurso desagradable, que va desde la quema de la bandera en público hasta las chaquetas adornadas con *F-bombs* en los juzgados[421].

Espacios para la expresión. Consiste principalmente en los "foros públicos tradicionales" y sus equivalentes en la propiedad privada. Se incluyen los parques públicos, calles y plazas. Su importancia radica tanto en la relación de la población con ellos y el área espacial que cubren.[422] A diferencia de otros espacios, los foros públicos tradicionales no pueden ser cerrados por completo al discurso público[423].

Espacios democráticos. Se asegura que algunos de los oradores accedan a espacios necesarios para que la democracia funcione:

"cualquier expresión o debate en cualquiera de las Cámaras, no podrá ser cuestionada en ningún otro lugar."

---

qué libros puede leer o qué películas ver". Idem, referencia 169, citando a su vez *Stanley*, 394 U.S. at 565-66. Ver también *Osborne vs. Ohio*, 495 U.S. 103 (1990) (confirmando el procesamiento para la tenencia de pornografía infantil (no virtual).

[418] Idem, p. 30, referencia 173, citando a su vez *Rowan vs. Post Office Dept*., 397 U.S. 728 (1970).

[419] Idem, referencia 174, citando a su vez *FCC vs. Pacifica Foundation*, 438 U.S. 726, 748-749 (1978).

[420] Idem, referencia 175, citando a su vez *Kovacs vs. Cooper*, 336 U.S. 77, 86-87 (1949).

[421] Idem, referencia 177, citando a su vez *Texas vs. Johnson*, 491 U.S. 397, 414 (1989); *Cohen vs. California*, 403 U.S. 15, 21-22 (1971).

[422] Idem, p. 30.

[423] En *Hague vs. Committee for Industrial Organization*, resuelto en 1939 el Tribunal anuló una ordenanza prohibiendo la actividad panfletaria "en cualquier calle o lugar público". El Tribunal también ha anulado leyes que prohibían panfletos en lugares públicos. Similares reflexiones desde un punto de vista arquitectónico, cualquier restricción que no sea una prohibición, "debe dejar abiertos otros amplios canales alternativos para la comunicación". Idem, referencia 182, citando a su vez *Perry Educ. Ass'n*, 460 U.S. at 45, 56 (énfasis añadido por Ammori).

En términos de espacios suficientes para el habla, los espacios del Congreso son tan necesarios para la democracia como la protección de los hogares de los estadounidenses.[424]

III.2.2.1.b.2. Segundo Principio: de los espacios adicionales. Basada en los espacios anteriores, la Corte Suprema proporciona una considerable aunque circunscrita deferencia a las iniciativas gubernamentales para abrir espacios, públicos o privados, físicos o virtuales. Además, los gobiernos pueden crearlos para determinados tipos de oradores según objetivos más específicos, como para incentivar la educación o la política. Los tribunales circunscriben esta deferencia, estableciendo que el gobierno no debe castigar o discriminar mensajes a través de la apertura de estos espacios.[425]-[426]

Espacios físicos: de propiedad pública y de propiedad privada.

Espacios físicos de propiedad pública. El gobierno puede abrir espacios de su propiedad para la expresión, estableciendo los tribunales que una vez abierto el espacio, este debe ser tratado como foro público tradicional.[427].

Espacios físicos de propiedad privada. También puede designar este tipo de espacios para la expresión, siempre y cuando el espacio sea lo suficientemente abierto para el público y el gobierno actúe con neutralidad de contenido.[428]

Espacios virtuales: de propiedad pública y de propiedad privada.

---

[424] Idem, p. 31.
[425] Idem, p. 32.
[426] La deferencia para con los espacios adicionales, promueve más expresión de dos maneras. Primero, el gobierno puede dar acceso a más espacios de discurso. En segundo lugar, la cuestión de la propia arquitectura comunicativa de la sociedad se convierte en un adicional tema legítimo del debate democrático. Idem, p. 33.
[427] Idem, p.33.
[428] En 1980, en *Pruneyard Shopping Center vs. Robins*, la Corte Suprema sostuvo por unanimidad que los Estados pueden adoptar una legislación que abra centros comerciales privados para el habla. Idem.

Espacios virtuales de propiedad del gobierno. A lo largo de casi toda la historia de EE.UU., su red postal ha sido el principal espacio virtual para la expresión. Así como hoy los periódicos están disponibles a través del ciberespacio, en un principio estaban disponibles a través de "espacios" postales. La protección y promoción de la expresión de los periódicos ha informado la historia de Estados Unidos aún más que la doctrina judicial.[429]-[430]-[431]

Hoy las revistas políticas circulan con bajas tarifas postales, el mayor cliente corporativo de la red postal es *Netflix*, que distribuye películas y programas tanto a través del servicio postal como de la Internet. Le es necesario el acceso a dos espacios virtuales de expresión: el acceso postal a través de las tarifas postales y la Internet a través de la neutralidad de la red.[432]

Espacios virtuales de propiedad privada. Se han designado varios espacios, como lo ha hecho dentro de los espacios físicos al designar centros comerciales. Estos incluyen, entre otros[433], los sistemas de cable, los sistemas de telefonía y los de acceso a Internet:

---

[429] Idem, p. 34 y 35.

[430] Desde antes de la Constitución y hasta bien entrado el s. XX correos y la prensa trabajaban juntos como un sistema de comunicación. Hoy, en palabras del juez Brennan, el servicio postal es "un medio nacional vital de expresión". Función principal de la red postal fue la difusión de la prensa. Los nombres de los periódicos todavía reflejan esta relación: el "*Evening Post"* o el "*Daily Mail*".Idem, p. 35.

[431] La política de no discriminación del Congreso abrió espacios para todos los periódicos, revocando la práctica pre–Constitucional según la cual los administradores de correos negarían acceso postal a *papers* según su discrecionalidad, como los operadores de cable de hoy, que podrían determinar hasta cierto punto que canales exhiben o abandonan. Idem, p. 36.

[432] Idem.

[433] También se regula el acceso a los espacios de radiodifusión. En la controvertida decisión de *Red Lion*, el Tribunal confirmó el acceso de los individuos atacados personalmente a replicar. En otra decisión, la Corte Suprema confirmó una norma de la *FCC* otorgando un "acceso razonable" a emitir espacios a los candidatos federales. El Tribunal sostuvo que la norma "equilibra adecuadamente los derechos de la Primera Enmienda de los candidatos federales, del público y de los organismos de radiodifusión", y "hace una contribución significativa a la libertad de expresión mediante la mejora de la capacidad de los candidatos para presentar, y del público para recibir la información necesaria para el funcionamiento eficaz del proceso democrático". Idem, ver referencia 270 y 272, que citan a su vez *Red Lion Broad. Co. v. FCC*, 395 U.S. 367, 375 (1969) y *CBS, Inc. v. FCC*, 453 U.S. 367, 394-96 (1981) y 396-97.

Acceso a los sistemas de cable. Parecido a un foro público designado, el gobierno federal impone al portador común como requisito llevar los canales propiedad de terceros que pagan una cuota para el transporte.[434]

Además, los estados pueden requerirles ofrecer acceso a diferentes tipos de altavoces, como: canales de acceso público, para todos los residentes, y canales educativos y gubernamentales.[435]

Acceso a espacios satelitales. El congreso ha ordenado a la *FCC* requerirles a los operadores satelitales que dejen entre el cuatro a siete por ciento de su capacidad a altavoces específicos: canales sin fines de lucro, educativos o informativos. El Circuito *D.C.* mantuvo la regla.[436]

Los sistemas telefónicos y los sistemas de acceso a la Internet. Durante los últimos veinte años las empresas de telefonía han hecho numerosas alegaciones de Primera Enmienda contra su regulación, raramente contra la que establece acceso no discriminatorio en su servicio de voz, ya que se sabe inviable. Por el contrario, desafían la normativa aplicable a las nuevas tecnologías, como su oferta de televisión por cable y de servicios de Internet. La *FCC* impuso recientemente reglas de neutralidad de red en alguna de las licencias de *Verizon Wireless*, a pesar de las vigorosas alegaciones de Primera Enmienda hechas por esa compañía a la *FCC*, antes de abandonarlas en sede judicial[437]. A pesar del mito de que la Internet es un espacio no regulado, la regulación ha sido fundamental para la designación de espacios en Internet

[434] Idem, p. 39.
[435] Una resolución desde el Circuito de *D.C.*, los jueces Anthony Kennedy y Ruth Bader Ginsburg argumentaron que los canales de acceso público deben ser tratados como foros públicos designados, a pesar de que los espacios sean sistemas de cable de propiedad privada. Idem, referencia 249, citando a su vez *Denver Area Educ. Telecomms. Consortium, Inc. vs. FCC*, 518 *U.S.* 727, 791-92 (1996).
[436] Idem, referencia 251, citando a su vez *Time Warner Entm't Co. v. FCC*, 93 F.3d 957, 975-76 (*D.C. Cir.* 1996).
[437] Idem, p. 39 y 40, referencia 261, citando a su vez Grant Gross, *CTIA Drops Lawsuit Against FCC's Open Access Rules*, PC WORLD (Nov. 13, 2008 4:00PM), [en línea] <http://www.pcworld.com/businesscenter/article/153848/ctia_drops_lawsuit_against_fccs_open_access_rules.html> [Consulta: 09/09/2013].

para todos los oradores. En concreto, y sin objeción constitucional, el gobierno garantiza el acceso de todos a utilizar cualquier proveedor de servicios *dial - up* de Internet. Esto incluye el derecho de acceso telefónico a un *ISP* que dé a los usuarios el acceso a la totalidad de la Internet, en lugar de acceso ISP a un "jardín amurallado", o contenidos preferidos por la compañía telefónica o de cable. Desde 2005, a través de declaraciones, acciones de ejecución y, finalmente, reglas, la *FCC* ha impuesto requisitos de neutralidad de la red[438].

III.2.2.1.b.3. Tercer Principio: de las fuentes diversas y antagónicas. El Poder Judicial también ha promovido la diversidad de las fuentes permitiendo al gobierno promover espacios discrecionales.[439] Además, la Corte Suprema ha sostenido que el Congreso y la *FCC* pueden fomentar la diversificación de las fuentes basándose no en la ley antimonopolio, sino que en las motivaciones de la Primera Enmienda.[440]

El Tribunal Supremo ha afirmado en variadas ocasiones que el "principio básico" de la Primera Enmienda es que la democracia estadounidense se basa en la:

"más amplia difusión de la información a partir de fuentes diversas y antagónicas"[441].

El juez Learned Hand, ha declarado que la nación estadounidense se ha "arriesgado" por este principio básico y que el objetivo de la Primera Enmienda no es el de proteger los intereses de los periódicos como oradores, sino que el de garantizar:

"la difusión de noticias desde tantas fuentes diferentes y con tantas facetas y colores diferentes como sea posible"[442].

---

[438] Idem, p. 41, referencia 269, citando a su vez *Preserving the Open Internet*, *FCC* 10-201, 2010 *WL* 5281676, 43–115 (Dec. 23, 2010).
[439] Idem, p. 41 y 42.
[440] Idem, p. 42.
[441] Idem, referencia 275, citando a su vez *Associated Press v. U.S.*, 326 *U.S.* 1, 20 (1945).

El Tribunal Supremo ha declarado asimismo, que:

"asegurar que el público tenga acceso a una multiplicidad de fuentes de información" es un "propósito gubernamental de primer orden, ya que promueve los valores centrales de la Primera Enmienda"[443].

En coherencia con ello, la judicatura respalda dos grandes categorías de normas de diseño discrecionales: las reglas de acceso y los límites a la propiedad.

Respecto a las reglas de acceso, por ejemplo, las normas de transporte telefónico y de Internet buscan aumentar la diversidad de los oradores en espacios virtuales. Lo mismo las reglas de acceso postal, que dieron lugar a que ciudades tuviesen varios periódicos de propiedad independiente y no sólo los periódicos preferidos por el administrador de correo.[444]

Respecto a los límites a la propiedad. En la década del `40, se obligó a *NBC* a desprenderse de una de sus dos cadenas de radio nacionales. La Corte Suprema rechazó el argumento de la Primera Enmienda de la *NBC*[445]. En 1978 la Corte Suprema confirmó por unanimidad una norma que prohíbe a los periódicos la compra de emisoras en la misma localidad, sosteniendo explícitamente que su decisión no iba sólo en dirección a limitar la propiedad, sino que se promovían los valores de la Primera Enmienda, en particular la disponibilidad de diferentes fuentes[446]-[447].

---

[442] Idem, referencia 276, citando a su vez *United States v. Associated Press*, 52 F.Supp. 362, 372 (S.D.N.Y.1943).
[443] Idem, referencia 277, citando a su vez *Turner Broadcasting System, Inc. v. FCC* - 512 *U.S.* 622 (1994)
[444] Idem, p. 42 y 43.
[445] Idem, referencia 289 citando a su vez *Nat'l Broad. Co. v. United States*, 319 *U.S.* 190, 206-08, 224-27 (1943).
[446] Idem, p. 44, referencia 290, citando a su vez *FCC v. Nat'l Citizens Comm. for Broad*., 436 *U.S.* 775,797-802 (1978).
[447] Para la televisión por cable el tribunal del circuito *D.C.* estableció los límites legales para la propiedad horizontal y vertical. El Congreso justificó estas limitaciones basándose en el objetivo de la promoción de diversas fuentes. Idem, p. 44.

III.2.2.1.b.4. Cuarto principio: espacios para generación de expresión nacional y local. Los distintos gobiernos estadounidenses han intervenido el mercado de las comunicaciones tanto para promover la expresión, unificar las políticas nacionales, como para promover espacios para el discurso netamente local. La doctrina jurídica, dice Ammori, ha pasado generalmente por alto estas numerosas leyes y políticas.[448]-[449]

Espacios para la formación del discurso nacional. Desde el primer Congreso la política postal ha incentivado todos los ciudadanos tuvieran acceso a las noticias nacionales. En primer lugar, el gobierno incentivó el libre "intercambio de *papers*", con el que los editores del *Pennsylvania Chronicle* podían recibir noticias y artículos de la *South Carolina Gazette* o del *Maryland Journal*. En segundo lugar, el gobierno invirtió fuertemente en las rutas postales hasta los confines más remotos del país.[450]

Espacios locales. Para los periódicos locales, el gobierno ha adoptado precios muy bajos para el correo local. La política de radiodifusión ha sido similar. Las licencias de televisión abierta fueron asignadas con el objetivo principal de garantizar al menos una salida, incluso para las pequeñas comunidades locales. La política en telefonía ha buscado constantemente bajar los costos de las llamadas locales. [451]

[448] Idem, p. 45.
[449] La preocupación por los espacios nacionales y locales comenzó con los debates para la ratificación constitucional. Los redactores de la Constitución se enfrentaron a lo que el filósofo político Robert Dahl consideró para ese entonces nuevo reto: hacer que la democracia funcione para una gran nación diversa. Los modelos principales para las democracias estaban estrechamente ligados a las ciudades-estado, en lugar de una propagación hacia trece estados. Al mismo tiempo, había que preservar la autonomía local apreciada por trece estados independientes. Mientras que la estructura federal de la nación era una respuesta, otro fue la arquitectura legal de los espacios del habla para garantizar tanto los espacios nacionales como los locales. Idem.
[450] Idem, p. 45.
[451] Idem, p. 46 y 47.

III.2.2.1.b.5. Quinto principio: acceso universal. Permite que el gobierno actúe para asegurar que todos los estadounidenses tengan acceso a los espacios básicos de expresión.

El Tribunal Supremo afirma que la primera enmienda se basa en el supuesto de que la:

"más amplia difusión de la información" es esencial para una democracia[452].

El uso por parte del gobierno de los bienes públicos para el acceso universal es común y generalmente sin resistencias, como lo ya dicho sobre la implementación del acceso universal a los periódicos, invirtiendo en las oficinas de correos y rutas postales que atraviesan el país. En parte debido a tal política, antes del comienzo del s. XIX, los periódicos eran más comunes en EE.UU. que en cualquier otro lugar.[453]

Los gobiernos federal y estatal también impusieron obligaciones para la universalidad de acceso en otros espacios virtuales como el teléfono, la radiodifusión, la televisión satelital, por cable y la Internet. Existen políticas y procedimientos[454]-[455] de la *FCC* para la concesión de licencias en la telefonía celular que tienen como "objetivo principal" la "disponibilidad a nivel nacional del servicio". A propósito del acceso a Internet, el Congreso ha requerido a la *FCC* promover su expansión hacia todos los estadounidenses. Además, en la era del acceso telefónico, la *FCC* se negó a clasificar las llamadas a los proveedores de servicios de Internet lejanos como llamadas -entonces caras- de larga

[452] Idem, p. 47, referencia 322 citando a su vez *Associated Press v. U.S.*, 326 *U.S.* 1, 20 (1945).
[453] Idem, p. 47 y 48.
[454] Idem, p. 48, referencia 331 citando a su vez 47 *U.S.C.* § 254 (*Westlaw* 2011).
[455] Idem, p. 48, referencia 332 citando a su *vez Cellular Communications Systems*, 86 *F.C.C.*2d 469, 509 (1981), *modificada en* 89 *F.C.C.*2d 58 (1982).

distancia, sobretodo para garantizar el acceso más amplio de los espacios de la Internet.[456]

Observando los principios de la Primera Enmienda expuestos por el profesor Ammori entendemos como desde los albores de la República estadounidense sus fundadores buscaron generar una nación vinculada a través del lenguaje y expresión comunes respetando las comunidades locales, y consecuente a ello, fomentando la diversidad de fuentes y la circulación de la comunicación incentivando el debate y el debate diverso.

Nos queda ver qué actos comunicativos son, por excepción, rechazados por el constituyente estadounidense.

III.2.2.1.c. Excepciones a la Primera Enmienda.

Si bien como ya lo hemos observado, la Primera Enmienda dispone de protecciones muy amplias para la libertad de expresión en Estados Unidos, esta libertad no es absoluta. Por lo general, el gobierno tiene mayor arbitrio para imponer restricciones neutras en cuanto al contenido que restricciones en función del contenido.

Restricciones neutras en cuanto al contenido. El gobierno puede imponer restricciones de tiempo, lugar y modo en el ejercicio de la libertad de expresión, siempre y cuando estas restricciones no se basen en el contenido de la manifestación ni en el punto de vista del hablante. Además, estas restricciones deben ser *ad hoc* para atender un interés sustancial del gobierno y deben dejarse abiertos otros canales de comunicación[457]-[458].

[456] Idem, p. 49, referencia 346 citando a su vez *Connect America Fund*, *FCC* 10-90, 2011 WL 466775 (February 9, 2011).
[457]OFICINA DE PROGRAMAS DE INFORMACION INTERNACION DEL DEPARTAMENTO DE ESTADO DE LOS ESTADOS UNIDOS, *"La libertad de expresión en Estados Unidos"*. [en línea] <http://iipdigital.usembassy.gov/st/spanish/pamphlet/2013/04/20130419146174.html#axzz2gjCpr5p0>

Restricciones en función del contenido. Generalmente inadmisibles, existen algunas excepciones muy específicas. De conformidad con la Primera Enmienda, las categorías de expresión que pueden restringirse son: la incitación a actos violentos inminentes[459], las amenazas reales[460], las expresiones difamatorias[461] y la obscenidad[462], que si bien pueden restringirse para poder conseguirse ello se deben cumplir exigentes requisitos.

[Consulta 12/08/2013] cita 2 citando a su vez *Perry Educ. Ass'n contra Perry Educators' Ass'n*, 460 U.S. 37, 45 (1983).

[458] "Por ejemplo, el gobierno puede imponer reglamentaciones razonables al volumen de los altavoces que se utilicen en un distrito comercial del centro de una ciudad; puede imponer límites razonables a las manifestaciones en vecindarios residenciales en medio de la noche, o puede exigir permisos para desfiles y manifestaciones organizadas a fin de garantizar que no generen peligros para la seguridad pública, siempre y cuando tales restricciones tengan validez para todos los hablantes, independientemente del contenido o punto de vista particular del discurso." Idem.

[459] "Se podrá restringir la libertad de expresión de una persona si dicha expresión 1) tiene por objetivo incitar o generar conductas al margen de la ley, 2) existe la probabilidad de que incite semejantes conductas, y 3) existe la probabilidad de que estas conductas se produzcan de manera inminente. Este es un criterio muy estricto y en raras ocasiones los tribunales encuentran que se ha cumplido.

La propugnación general de la violencia, como por ejemplo escribir en un sitio *web* que la revolución violenta es la única solución para los problemas de la sociedad, no constituye incitación a actos de violencia inminentes.

Por ejemplo, en 1969, un miembro del *Ku Klux Klan* pronunció un discurso en Ohio en el que defendía la "revenganza" (sic) contra judíos y afroestadounidenses. El Tribunal Supremo de Estados Unidos derogó un estatuto que prohibía este discurso porque penalizaba las expresiones que no iban "dirigidas a incitar o producir conductas inminentes al margen de la ley" y que no tenían "la probabilidad de incitar o producir semejantes conductas".

De igual manera, si una persona quema una bandera de Estados Unidos en señal de protesta contra las políticas de inmigración del gobierno y un manifestante opositor se altera y ataca físicamente a alguien que parece ser un inmigrante, es probable que la libertad de expresión de la persona que quemó la bandera esté protegida por la Primera Enmienda, ya que no tenía la intención de incitar a la violencia.

Por el contrario, si un orador que pertenece a un grupo étnico en particular exhorta a una turba a atacar de manera inminente y física a una persona de otro grupo étnico para demostrar su superioridad, y una persona de dicho grupo agrede físicamente a una persona del otro grupo étnico, es probable que el discurso del orador no esté protegido por la Primera Enmienda, ya que pretendía incitar a actos violentos inminentes y probablemente incitaría a tal violencia". Oficina de programas (…), op. cit.

[460] Se trata de una declaración en la que el receptor de la comunicación asumiría de manera razonable que el hablante, o las personas que trabajan con él, pretenden causar daño físico al receptor. Idem.

[461] Consisten en declaraciones falsas que vulneran el carácter, la fama o la reputación de una persona. Debe tratarse de una manifestación falsa de los hechos; es decir, la manifestación de opiniones, por insultantes que sean, no constituye difamación. Se utilizan distintos criterios para los funcionarios públicos y los particulares. En 1964, el Tribunal Supremo decretó que los funcionarios públicos podían probar la difamación solo si podían demostrar "mala voluntad real", es decir, que la persona actuó con conocimiento de que la afirmación difamatoria era falsa o con "imprudencia temeraria sobre si la declaración era falsa o no".

Aun cuando los tribunales determinen que hubo difamación, no imponen sanciones penales. Idem.

[462] Las obscenidades se pueden restringir de conformidad con la Primera Enmienda, pero se ha producido un prolongado debate sobre qué se considera obscenidad y cómo se debe regular. En 1973 el Tribunal Supremo definió obscenidad como una expresión que la persona promedio, que aplique las normas

A propósito de la protección de la seguridad nacional como categoría restrictiva de la libertad de expresión, la Corte Suprema ha reconocido el interés del gobierno en mantener alguna información secreta, como por ejemplo, los desplazamientos de las tropas en tiempos de guerra. Pero la Corte en realidad nunca ha planteado reproches contra la libertad de expresión basándose en la seguridad nacional.[463] De este hecho histórico se pueden aprender dos lecciones. Primero, la cantidad de expresión que podría limitarse en interés de la seguridad nacional sería muy limitada. Segundo, históricamente el gobierno se ha excedido en el uso del concepto de "seguridad nacional" para protegerse de la crítica y desalentar el debate de políticas o decisiones controversiales.[464]

Hemos visto que la protección de la seguridad nacional no es una excepción propiamente tal a la libertad de expresión, sin embargo la historia nos presenta el establecimiento de leyes o los requerimientos judiciales de restricción a la libertad de expresión y de prensa fundados en aquel bien jurídico. Para ello debemos entonces hacernos cargo de revisar doctrinas generadas a través de décadas por el Tribunal Supremo estadounidense, entendiendo que ellas se encuentran incorporadas a la Primera Enmienda a través de precedentes, hablamos de la doctrina de la censura previa y la de las sanciones *expost*.

III.2.2.1.d. Doctrina de la censura previa. Primero cabe responder ¿Qué es la censura previa? Ella se refiere a restricciones oficiales impuestas a la

---

sociales modernas, encuentre que 1) recurre a intereses lascivos, 2) representa o describe una conducta sexual de manera claramente ofensiva, y 3) carece de valor literario, artístico, político o científico, cuando se considera en su conjunto.
Los tribunales valoran de manera independiente cada elemento y no clasifican la expresión como obscena a menos que se cumplan todos los factores. Por ejemplo, si un libro utiliza lenguaje soez y describe conductas sexuales pero, en su conjunto, no recurre a intereses lascivos o tiene valor literario, no se considera obsceno. Debido a criterios tan estrictos, no es común que los tribunales determinen como obscena una expresión. Idem.

[463] Lo que debemos distinguir de la aplicación de la ley de espionaje, pues el espionaje en sí mismo no es expresión sino que la consecución de actos para obtener información clasificada por medios ilícitos.

[464] AMERICAN CIVIL LIBERTIES UNION, *"Libertad de expresión"*, [en línea] <https://www.aclu.org/libertad-de-expresion> [Consulta 12/08/2013]

expresión en sus diversas formas antes de que esta se lleve a cabo o se publique. La censura previa se distingue así del castigo posterior, que es una sanción impuesta después que la comunicación ha sido hecha, como un castigo por haberlo realizado. [465]

Un sistema de censura previa impide que la comunicación se produzca en términos absolutos. Un sistema de castigo posterior permite la comunicación, pero impone una sanción posterior. El efecto disuasorio de la sanción posterior puede operar evitando la comunicación o mitigando una expresión una vez ya hecha. Sin embargo, el impacto en la libertad de expresión puede ser bastante diferente, dependiendo de si el sistema de control está diseñado para bloquear la publicación de antemano o disuadir con un castigo.[466]

El primer encuentro del Tribunal Supremo con una ley que impuso una restricción previa fue en *Near v. Minnesota ex rel. Olson (1931)*, en el que se resolvió anular una ley que autorizaba a imponer aquellas restricciones permanentemente ante publicaciones "obscenas, lascivas y lujuriosas" o "malévolas, escandalosas y difamatorias". Ello, después de que un periódico imprimiendo una serie de artículos que asociaba funcionarios locales a gángsteres:[467]

"[La] administración del gobierno se ha hecho más compleja, las oportunidades para la corrupción se han multiplicado, el crimen se ha expandido a dimensiones más serias, y el peligro de que este sea protegido por funcionarios desleales y que el daño a la seguridad fundamental de la vida y de la propiedad sea llevado a cabo por alianzas criminales y negligencia oficial,

[465] EMERSON, Thomas I. *"The doctrine of prior restraint"*. [La doctrina de la censura previa]. 1955, Yale Law School Legal Scholarship Repository, p. 648.
[466] Idem.
[467] U.S. GOVERNMENT PRINTED OFFICE (GPO), *"First amendment. Religion and Expression"*. [Primera Enmienda. Religión y Expresión], p. 1029, cita 43, citando a su vez *Near v. Minnesota ex rel. Olson*, 283 *U.S.* 697, 716 (1931).

acentúan la necesidad primaria de una prensa vigilante y valerosa, sobre todo en las grandes ciudades"[468].

"La libertad de prensa, históricamente considerada y adoptada por la Constitución Federal, ha significado, sobre todo, aunque no exclusivamente, inmunidad a restricciones previas o censura"[469]. "Cualquier sistema de restricción previa a la expresión que llegue a este Tribunal contiene una pesada presunción contra su validez constitucional"[470].

En *Nebraska Press Ass'n. v. Stuart (1976)* se da un conflicto entre la libertad de prensa y las garantías procesales. La Corte decidió por unanimidad dejar sin efecto una orden judicial estatal de restricción a la publicación de información que pudiese perjudicar el posterior juicio de un acusado.[471]

El más reciente encuentro de la Corte con la doctrina en materia de seguridad nacional, se produjo cuando el gobierno en *New York Times Co. vs. United States (1971)* también conocido como el caso de los *"Pentagon Papers"* trató de prohibir la publicación de prensa de documentos clasificados relacionados con la guerra de Vietnam. Si bien el Tribunal rechazó el intento de censura previa, algunos de los jueces estuvieron de acuerdo en el que la restricción previa de las publicaciones sería constitucional si se sobrepasa el test del "peligro claro y presente".

Por lo tanto, la doctrina de la censura previa de la Corte Suprema estadounidense justamente está fundamentada en el principio general de la primera enmienda, constituyendo un gran obstáculo a superar por quienes pretendan censurar. Ahora si bien este principio general de la Primera Enmienda, de la libertad de expresión, se ha mantenido vigente, se extraña una

[468] Op. cit, p. 1030, cita 50, citando a su vez *Near v. Minnesota* (1931).
[469] Idem, p. 1030, cita 51.
[470] Idem, cita 44, citando a su vez *Bantam Books v. Sullivan*, 372 *U.S.* 58, 70 (1963).
[471] Op. cit., p 1031, cita 56, citando a su vez *Nebraska Press Ass'n. v. Stuart*, 427 *U.S.* 539 (1976).

doctrina de la censura previa más exhaustiva, coherente en sus aplicaciones y excepciones, estamos a la espera de que surja[472].

Ahora, aunque el contexto del caso *Wikileaks* no es el de la censura previa, no queremos que preguntas atingentes que van surgiendo queden sin responderse:

III.2.2.1.d.1. Doctrina del peligro claro y presente. Es la doctrina nacida en la Primera Guerra Mundial mediante la cual, según algunos, se podrían establecer límites a la Primera Enmienda en relación a los derechos a la libertad de expresión y de prensa de cumplirse las condiciones que establece. Para su estudio utilizaremos la observación en su voto concurrente del juez Douglas en la decisión de la Corte Suprema para *Brandenburg v. Ohio* (1969), siendo de interés subrayar la época en que estos planteamientos son realizados, cercanos a la experiencia de la segunda guerra y previas al gran caso a favor de la libre expresión y prensa, los *Pentagon Papers*[473]:

"La prueba del "peligro claro y presente" fue concebida por el juez Holmes en un caso que surgió durante la Primera Guerra Mundial, una guerra declarada por el Congreso, no por el Ejecutivo. El caso fue *Schenck v. United States (1919)*[474], en el que una persona fue acusada de intentar causar una insubordinación en las fuerzas militares y obstaculizar el alistamiento. Se distribuyeron panfletos que instaban a resistirse al enrolamiento obligatorio, denunciaban la conscripción e impugnaban los móviles de quienes respaldaban la iniciativa bélica. La Primera Enmienda fue citada como defensa. El juez Holmes, en rechazo de dicha defensa, expresó:

[472] Op. cit., p. 1030 y 1031.
[473] Brandenburg v Ohio. Traducción obtenida [en línea] <http://www.palermo.edu/cele/libertad-de-expresion/jurisprudencia/pdf-eeuu/BRANDENBURG-v OHIO,395-U.S.pdf> [Consulta: 9/10/2013]
[474] 249 U.S. 47, 52.

"En todos los casos, la cuestión es si los términos utilizados se emplean en tales circunstancias y son de tal naturaleza que pueden generar el peligro claro y presente de que se produzcan los daños graves que el Congreso tiene derecho a prevenir. Es una cuestión de proximidad y medida".

El segundo caso fue *Frohwerk v. United States (1919)*, cuya resolución también corresponde al juez Holmes, implicó el juicio y castigo de la publicación de artículos que criticaban duramente la iniciativa bélica en la Primera Guerra Mundial. Se hizo referencia al caso *Schenck* como ejemplo de una condena aplicada por obstrucción de la seguridad "a través de un discurso persuasivo"(…). La condena se confirmó porque:

"el periódico circulaba en lugares donde una pequeña chispa bastaba para encender una llama".

Debs v. United States (1919) fue el tercer caso de la trilogía del 19. Debs fue condenado por manifestarse en oposición a la guerra, en tanto su:

"oposición se expresó de tal manera que su efecto natural y esperado hubiera sido obstaculizar el reclutamiento".

"Si esa fue la intención y si, en todas las circunstancias, ese hubiera sido su probable efecto, no gozaría de protección por formar parte de un programa general ni por ser la expresión de una creencia general y consciente".

En 1919 la Corte aplicó la doctrina *Schenck* para ratificar condenas a otros disidentes en la Primera Guerra, *Abrams v. United States (1919)*, fue uno de estos casos. Sin embargo aquí el juez Holmes expresó una opinión disidente, a la cual se sumó el juez Brandeis (…) No consideraba que se hubieran expuesto argumentos suficientes para desestimar la Primera Enmienda en relación con los antecedentes de hecho:

"Solamente el peligro actual de un mal inmediato o de una intención de causarlo justifica el hecho de que el Congreso limite la expresión de opiniones en casos en que no haya derechos privados involucrados. Ciertamente el Congreso no puede prohibir todos los esfuerzos por modificar la mentalidad del país".

Otro ejemplo de esta situación fue el caso *Schaefer v. United States (1920)*, donde el juez Brandeis expresó una opinión disidente, secundada por el juez Holmes. Y un tercer ejemplo fue el caso *Pierce v. United States (1929)*, en el cual el juez Brandeis expresó un voto disidente, al que adhirió el juez Holmes.

Esos fueron los casos de la Primera Guerra Mundial que añadieron la condición de "peligro claro y presente" en la Primera Enmienda."

Luego el juez Douglas se hace una pregunta estableciendo un punto:

"Si el poder de la guerra resulta adecuado para sostener esa doctrina es una cuestión discutible[475].

Luego, subraya que "El disenso en *Abrams, Schaefer* y *Pierce* muestra con qué facilidad se manipula el "peligro claro y presente" para frustrar lo que Brandeis denominó:

"el derecho fundamental de los hombres libres a luchar por mejores condiciones a través de nueva legislación y nuevas instituciones", mediante la argumentación y el discurso[476].

Para terminar el punto, Douglas razona que:

"Si bien dudo de que la prueba del "peligro claro y presente" sea coherente con la Primera Enmienda en tiempos de guerra declarada, estoy seguro de que no puede conciliarse con la Primera Enmienda en tiempos de paz."

Agrega que "el juez Holmes, aunque nunca abandonó formalmente la prueba del "peligro claro y presente", se acercó al ideal de la Primera Enmienda cuando expresó su disidencia en el caso *Gitlow v. New York(1925)*[477]-[478]

[475] *Brandenburg v. Ohio (1969)* [395 U.S. 444, 452].
[476] *Pierce v. United States*, 273.
[477] 268 U.S. 652, 673: "Cada idea constituye una incitación. Se ofrece para que los demás la crean y, de ser así, esa idea se convierte en un fundamento para la acción, salvo que sea superada por otra creencia, o

En el caso *Bridges v. California (1941)*, se aprobó la prueba del “peligro claro y presente” en un *dictum* detallado que acotó su alcance y la situó en una categoría más delimitada. Pero en el caso *Dennis v. United States (1951)*, se abrió ampliamente esa puerta y se distorsionó la prueba del “peligro claro y presente” hasta los límites de lo reconocible[479].

Comenzando a finalizar su interesante e importante análisis, observó: “No creo que en el régimen de la Primera Enmienda haya lugar para la prueba del “peligro claro y presente”, ni estricta y severa, como la preferirían algunos, ni flexible como la reformuló la Corte en el caso *Dennis*.

Cuando uno lee detenidamente las opiniones y ve cuándo y cómo se aplicó la prueba del “peligro claro y presente”, se suscitan grandes dudas. En primer lugar, si bien las amenazas muchas veces sonaron fuerte, siempre fueron endebles, y solamente fueron tomadas en serio por jueces tan atados al *statu quo* que se mostraban nerviosos ante la posibilidad de realizar un análisis crítico. En segundo lugar, la prueba en el caso *Dennis* era tan retorcida y perversa que permitió que el juicio a esos predicadores del marxismo se transformara en un juicio absolutamente político que formó parte esencial de la

---

que una falta de ímpetu sofoque el movimiento apenas iniciado. La única diferencia entre la expresión de una opinión y una incitación en el sentido más acotado del término es el entusiasmo que el orador tenga en el resultado. La elocuencia puede aniquilar a la razón. Sin embargo, cualquiera sea la opinión que se tenga del discurso excesivo que tenemos frente a nosotros, no tenía posibilidades de iniciar una conflagración en ese momento. Si, a largo plazo, las creencias expresadas en una dictadura proletaria están destinadas a ser aceptadas por las fuerzas dominantes de la comunidad, el único sentido de la libertad de expresión es que tales creencias deben tener su oportunidad y su espacio para manifestarse".

[478] En el caso *Herndon v. Lowry*, 301 *U.S.* 242, la Corte revocó una condena que sancionaba la invocación de los derechos consagrados en la Primera Enmienda con el fin de instigar a una insurrección debido a que no existían pruebas suficientes de dicha instigación. Ver también *Hartzel v. United States,* 322 *U.S.* 680.

[479] En ese caso, la acusación había calificado de "conspiración" a un acuerdo para predicar el marxismo. El caso fue sometido a un jurado con la condición de que este no podía imponer una condena a menos que determinara que los acusados “se proponían derrocar al Gobierno 'tan pronto como las circunstancias lo permitieran'”. La Corte confirmó las condenas por esa imputación e interpretó que significaba.
Ver McKay, *The Preference For Freedom*, 34 *N. Y. U. L. Rev*. 1182, 1203-1212 (1959) una determinación de "si la gravedad del "mal", teniendo en cuenta su improbabilidad, justifica una invasión de la libertad de expresión tal como la que resulta necesaria para evitar el peligro'". Cita de *United States v. Dennis*, 183 F.2d 201, 212.

Guerra Fría y que ha erosionado importantes pasajes de la Primera Enmienda"[480].

Por último, hace mención al único caso en el que desde su perspectiva cabe sancionar la libertad de expresión: "El ejemplo que habitualmente dan quienes estarían dispuestos a condenar una expresión es el caso de una persona que, en un teatro abarrotado de espectadores, grita a viva voz que se está produciendo un incendio cuando ello no es cierto. Este es, no obstante, un clásico caso en el cual el discurso está unido a la acción[481]. De hecho, son inseparables y es posible juzgar a quienes efectivamente realizan estos actos manifiestos[482]. Más allá de los casos poco frecuentes de este tipo, el discurso, en mi opinión, no puede ser sometido a juicio."

III.2.2.1.e. Eventuales sanciones ex post. El contexto de la controversia sobre la libertad de expresión al momento de la ratificación de la Primera Enmienda era la censura previa. Pero la mera exención a restricciones preventivas no puede ser todo lo que este garantizado por las disposiciones constitucionales, pues la libertad de la prensa podría traducirse en una burla y un engaño, si, cada uno estando en la libertad de publicar lo que quisiera,

[480] "Las creencias de una persona, durante mucho tiempo, se consideraron espacios sagrados que el gobierno no podía invadir. El caso *Barenblatt* es un ejemplo de la facilidad con que puede violarse dicho espacio sagrado. La separación que estableció la Corte entre el acto delictivo de ser un comunista "activo" y el acto inocente de ser comunista en teoría o inactivo marcan la diferencia únicamente entre la creencia profunda y perdurable y la creencia casual o incierta. Pero yo creo que todas las cuestiones que tienen que ver con creencias están más allá del alcance de las citaciones judiciales o de los sondeos de los investigadores. Por eso, las invasiones de la privacidad perpetradas por los comités investigadores fueron claramente inconstitucionales. Esa es la profunda falla de las tristemente célebres audiencias sobre lealtad y seguridad que, desde 1947 —año en que el presidente Truman las instauró— han procesado a 20.000.000 de hombres y mujeres. Esas audiencias tuvieron que ver, fundamentalmente, con los pensamientos, las ideas, las creencias y las convicciones de las personas. Constituyeron las más flagrantes violaciones de la Primera Enmienda de las que hayamos tomado conocimiento." *Brandenburg v. Ohio (1969)*.

[481] Ver *Speiser v. Randall (1958)*.

[482] *Brandenburg v. Ohio (1969)*.

estuviese afecto a que las autoridades públicas pudieran, sin embargo, castigarlo por publicaciones inofensivas.[483]

El mal que se puede prevenir no es sólo el de la censura de la prensa, sino que también toda acción del gobierno por medio de la cual se intente evitar tales discusiones libres de los asuntos públicos como parece absolutamente esencial para preparar a la gente para un ejercicio inteligente de sus derechos como ciudadanos.[484] Un Estado de Derecho que permita imponer responsabilidad penal o civil a los que hablen o escriban sobre temas de interés público daría lugar a la autocensura, lo que no sería aliviado permitiéndose una defensa de la verdad. Una norma así, disminuiría el vigor y limitaría la variedad del debate público.[485]

> "Los que ganaron nuestra independencia creían que el fin último del Estado era hacer a los hombres libres de desarrollar sus facultades, y que en su gobierno las fuerzas deliberantes deben prevalecer sobre lo arbitrario. Ellos valoraban la libertad como fin y como medio. Creían que en la libertad de ser estaba el secreto de la felicidad y en el coraje de ser el secreto de la libertad. Ellos creían que la libertad de pensamiento y expresión eran medios indispensables para el descubrimiento y la difusión de la verdad política, que sin libertad de expresión no habría debate (…) que la mayor amenaza a la libertad es un pueblo inerte, que la discusión pública es un deber político, y que esto debe ser un principio fundamental del gobierno estadounidense (…)"[486].

II.2.3. La Ley de Fraude Informático.

[483] U.S. government printed (…), op. cit., p. 1034.
[484] Idem, p. 1034, cita 70, citando a su vez a Cooley, T. *"A treatise on the constitucional limitations which rest upon the legislative powers of the states of the american union"*. (8va. ed. 1927).
[485] Idem, cita 71, citando *New York Times Co. v. Sullivan*, 376 *U.S.* 254, 279 (1964). Ver también *Speiser v. Randall*, 357 *U.S.* 513, 526 (1958); *Smith v. California*, 361 *U.S.* 147, 153–154 (1959); *Time, Inc. v. Hill*, 385 *U.S.* 374, 389 (1967).
[486] Idem, p. 1035 y 1036, cita 73 citando a su vez *Whitney v. California*, 274 *U.S.* 357, 375–76 (1927)

Al menos cuarenta leyes federales regulan diferentes delitos relacionados con la informática en los Estados Unidos. La principal ley federal que regula los delitos informáticos es la Ley de Fraude y Abuso Informático de 1986 (CFAA). La ley contiene una serie de disposiciones basadas en el acceso a una computadora sin autorización o excediendo el acceso autorizado. Se le critica gravemente que, ocupando una "metáfora de infracción" el concepto central de "acceso" no está definido y que, además no existe consenso judicial sobre su significado. Además en 1996 la Corte estatal de Kansas declaró nulo su concepto de acceso por su vaguedad [487].

Bajo este estatuto, siete categorías de conducta están prohibidas en su relación con "computadoras protegidas", que se definen como:

[Un] computador… utilizado por o para una entidad financiera o el gobierno de los Estados Unidos. . . o bien, que se utiliza para el comercio o las comunicaciones interestatales o externas, incluyendo un ordenador situado fuera de los Estados Unidos que se utilice de manera que afecte el comercio o las comunicaciones interestatales o externas de los Estados Unidos.[488]

En otras palabras, cualquier equipo en los Estados Unidos, que está conectado a la Internet, e incluso algunos equipos extranjeros están sujetos a la CFAA. La sección (a) (1) de la ley prohíbe la obtención o transmisión de información clasificada a través del acceso no autorizado al ordenador si existe "razón para creer" que la información podría ser utilizada ya sea en detrimento de los Estados Unidos, o en beneficio de cualquier nación extranjera[489]. En el

[487] CLOUGH, Jonathan. *"Data theft? Cybercrime and the increasing criminalization of acces to data"*. [¿Robo de datos? Ciberdelincuencia y la creciente criminalización del acceso a datos]. Criminal Law Forum (2011) 22:145–170, p. 155.
[488] HAMPSON, Noah C.N., *"Hacktivism: A new breed of protest in a networked world"*, [Hacktivismo: Una nueva generación de protesta en un mundo en red]. Boston College International and Comparative Law Review [Vol. 35:511 2012], p. 525, referencia 128 a propósito de la Computer Fraud and Abuse Act 18 U.S.C. § 1030(e) (2).
[489] COMPUTER FRAUD AND ABUSE ACT 18U.S.C. §1030(a) (1).

siguiente apartado se prohíbe la obtención de información financiera, de información de cualquier entidad gubernamental, o de información de cualquier "computadora protegida", a través del acceso no autorizado al ordenador[490]. En tercer lugar, la CFAA prohíbe el acceso no autorizado de cualquier equipo no público del gobierno de Estados Unidos[491]. En la sección (a) (4) prohíbe el acceso no autorizado al ordenador con la intención de defraudar y obtener una ganancia[492].

En la quinta subsección, § 1.030 (a) (5), se describen dos tipos de delitos. El primero consiste (A) provocar conscientemente la transmisión de un programa, información, código, o de comando, y como resultado de dicha conducta, provocar intencionadamente daños sin autorización, a un ordenador protegido. El segundo tipo de delito implica (B) acceder intencionalmente a un ordenador protegido sin autorización, y como resultado de esa conducta, imprudentemente causar daños, o (C) acceder intencionalmente a un ordenador protegido sin autorización, y como resultado de dicha conducta, causar daños y pérdidas.[493]

El sexto inciso prohíbe la obtención de contraseñas o de información similar con la intención de defraudar, accediendo sin autorización al computador afectando al comercio interestatal o externo, o si el equipo es utilizado por o para el gobierno de los EE.UU.[494]

Por último, el inciso § 1030 (a) (7) prohíbe la transmisión de información, con la intención de extorsionar. [495]

[490] 18U.S.C. §1030(a) (2).
[491] 18U.S.C. §1030(a)(3).
[492] 18U.S.C. §1030(a)(4).
[493] HAMPSON, op. cit. p. 526.
[494] Idem.
[495] Idem.

Las personas condenadas en virtud de estas disposiciones de la Ley de Espionaje están sujetas a penas de prisión y multa.[496]

III.2.4. La Ley de Espionaje.

La Ley de Espionaje de 1917, se basó en la Ley de Secretos de Defensa de 1911, que, como su nombre lo indica, criminaliza la divulgación de secretos relacionados con la defensa. La aprobación de esta ley fue una reacción a las máquinas de propaganda utilizadas con efectos dramáticos por las potencias europeas y los rebeldes rusos durante la Primera Guerra Mundial. Autoridades norteamericanas sostuvieron que el gobierno federal necesitaba nuevas y más amplias tácticas para restringir "la guerra de la propaganda". El Presidente Wilson estuvo de acuerdo, afirmando en un discurso ante el Congreso de la "necesidad de una legislación para reprimir actividades desleales." [497]

Con el propósito ostensible de abordar las preocupaciones de los militares, la ley pretendía criminalizar a quien "ponía en peligro la paz, el bienestar y el honor de los Estados Unidos". Después de nueve semanas de debate, el Congreso aprobó la legislación el 15 de junio de 1917.[498]

Mientras que en algunas de sus disposiciones la Ley de Espionaje criminaliza lo que tradicionalmente se entiende por espionaje o espionaje clásico, como el acceso no autorizado a la seguridad electrónica de instalaciones militares y la entrega a países extranjeros de información relacionada con la defensa, que pueda ser perjudicial para EE.UU.[499], diferentes

---

[496] 18U.S.C. §1030

[497] JONES, Shaina y Ward Brown, Jay, "*The Assange Effect: WikiLeaks, the Espionage Act and the Fourth Estate"*. [El Efecto Assange: WikiLeaks, la Ley de Espionaje y el Cuarto Poder]. En: Media Law Resource Center Bulletin, August, 2011, p. 124.

[498] Idem, p. 125.

[499] ESPIONAGE ACT 18 U.S.C. § 793 (a)-(b). JONES, p. 125.

a aquella calificación son las disposiciones de la Ley de Espionaje que suelen considerarse como potencialmente aplicables a *WikiLeaks.* Tales son[500]:

(c) El que "reciba u obtenga" de "cualquier persona o cualquier fuente" cualquier "información respecto a la defensa nacional, con intención o motivos para creer que la información se va a utilizar para la lesión de los Estados Unidos, o en beneficio de cualquier nación extranjera", sabiendo o teniendo razones para creer que la fuente de la información se suministra en violación de la ley.[501]

(e) el que tenga "posesión no autorizada de" un documento "relacionado con la defensa nacional" con "razones para creer que se podría utilizar para la lesión de los Estados Unidos o en beneficio de cualquier nación extranjera" y "voluntariamente comunique" a "cualquier persona que no tenga derecho a recibirla".[502]

(g) conspirar con otra persona para hacer cualquiera de lo anterior, si algún miembro de esta conspiración hace "cualquier acto para llevar a efecto el objeto de la conspiración".[503]

Las personas condenadas en virtud de estas disposiciones de la Ley de Espionaje están sujetas a penas de prisión y multa.[504]

III.3. ¿QUÉ DECISIONES HA TOMADO LA JURISPRUDENCIA ESTADOUNIDENSE DESDE LOS CASOS QUE LA DOCTRINA CONSIDERA SIMILARES Y RELEVANTES?

[500] JONES, op. cit., p. 117.
[501] 18 U.S.C. § 793 (c).
[502] 18 U.S.C. § 793 (e).
[503] 18 U.S.C. § 793 (g).
[504] JONES, op. cit., p.117.

III.3.1. A propósito de la Ley de Espionaje.

Teniendo en cuenta el origen de la Ley de Espionaje, no es de extrañar que la construcción significativa de sus términos en sede judicial se haya llevado a cabo durante la Segunda Guerra Mundial.[505]

III.3.1.1. Gorin v. Estados Unidos (1941). De Mikhail Gorin, ciudadano y agente de la U.R.S.S., se demostró que compró de un empleado de la Marina de EE.UU., Hafis Salich, información sobre las actividades japonesas en Estados Unidos[506]. Los informes se encontraban en los archivos de la oficina de Inteligencia Naval en San Pedro, California. Gorin y Salich fueron condenados por las prohibiciones penales clásicas contra el espionaje[507] y por conspiración.[508]

La Corte Suprema confirmó las condenas.[509]

Su importancia está en que nos establece los parámetros para reconocer el espionaje clásico.

III.3.1.2. Hartzel v. Estados Unidos (1944). La importancia de este caso está dada porque en él la Corte Suprema tuvo la oportunidad de esbozar el estándar requisito de procesamiento exitoso de esta ley.[510]

Elmer Hartzel no era un agente o un empleado del gobierno. En 1942, escribió tres artículos expresando su opinión negativa de la Segunda Guerra

[505] JONES, op. cit, p. 126.
[506] Actividades de funcionarios japoneses y civiles dentro de EE.UU., así como la vigilancia norteamericana de buques japoneses sospechosos de participar en actividades de espionaje. Idem.
[507] 18 U.S.C. § 793 (a)-(b). Mientras que por la mayoría se entiende que podrían eventualmente aplicarse a *WikiLeaks* las letras (c), (e) y (g).
[508] JONES, op. cit., p 126.
[509] Idem.
[510] Idem, p.127.

Mundial y de los aliados, entre otras cosas. Por ejemplo, en su folleto titulado "La médula espinal enferma", escribió fuertes expresiones criticando al presidente Roosevelt, distribuyéndolas en seiscientas direcciones pertenecientes a su lista de correo.[511]

La fiscalía afirmó que el actuar de Hartzel entraba en el ámbito de una disposición de la Ley de Espionaje que penalizaba causar o intentar causar "insubordinación, deslealtad, motín (…) en las fuerzas militares o navales de los Estados Unidos". El Tribunal Supremo dictaminó que el gobierno no había logrado cumplir el requisito de probar la intención en este caso. En consecuencia, la Corte anunció que,"[s]alvo que encuentren pruebas suficientes de que un jurado pudiese inferir más allá de una duda razonable de que tenía la intención de llevar a cabo las consecuencias específicas prohibidas por la ley, un ciudadano estadounidense tiene derecho a discutir estos temas, ya sea por medio de la razón templada o la inmoderación despiadada, sin violar la Ley de Espionaje de 1917".[512]

Debido a que Hartzel intentaba cambiar la opinión pública sobre la guerra sobre la base de sus opiniones personales, el Tribunal llegó a la conclusión de que no podía ser condenado.[513]

III.3.1.3. Estados Unidos v. Morison (1988). En este caso la Corte de Apelaciones de EE.UU. para el Cuarto Circuito examinó el alcance de la Ley de Espionaje en un contexto que está relacionado con la prensa.[514]

---

[511] Idem. Uno de sus escritos decía lo siguiente: "Wilson murió inválido, convirtiéndose Roosevelt en presidente. ¿Cuál es la importancia social de su condición?...Nuestro líder –a salvo en Washington- escapó de los horrores de la guerra, pero no pudo escapar del virus de la enfermedad de un niño. Al igual que con la sífilis su parálisis es indicativa de desajustes graves dentro de la nación. Se reproduce dentro de su cuerpo nuestra descomposición interna; de hecho él es un degenerado que ahora busca la manera de tenernos para sanarse. . . . Ocultos en el programa para salvar a la humanidad están los gérmenes del infantilismo, la parálisis y la muerte. Por ahora seguimos, no a un niño, sino que a un hombre con la enfermedad de un niño".

[512] Idem.

[513] Idem.

Samuel Morison era empleado del Centro de Apoyo de Inteligencia Naval y también trabajaba fuera de servicio como consultor de *Jane*, la editorial inglesa de varios periódicos relacionados con temas de defensa. Desde hace algún tiempo, Morison suministraba diversas fotografías e información a *Jane* con la aprobación de la Marina, pero sujeto al acuerdo de que no facilitaría información clasificada. Cuando sus servicios a los ingleses se convirtieron en una fuente de fricción con sus superiores navales, *Jane* lo entrevistó para un empleo permanente. Posiblemente, con la esperanza de obtener el trabajo, Morison envió fotografías clasificadas al editor en jefe, que la revista publicó. Mientras que a *Jane* nunca se le presentaron cargos, Morison fue acusado y condenado en virtud de, entre otras leyes penales, las secciones 793 (d) y (e). En su defensa, Morison intentó ser calificado como fuente de noticias, y argumentó que la ley no se le aplicaba porque no encajaba en el perfil de un "espía clásico". La Corte rechazó este argumento, señalando que los artículos por los que Morison fue procesado cubren más delitos que el del espionaje clásico, y que en virtud de estas secciones, la Ley se aplica correctamente a la divulgación de material clasificado a cualquier persona "que no tenga derecho a recibir" la misma.[515]

Por la misma razón, dos de los tres jueces que votaron por la condena de Morison lo distinguieron de la prensa, y en su conjunto la Corte señaló que, como empleado de inteligencia del gobierno, se le había puesto expresamente en su conocimiento el tenor de sus obligaciones en virtud de su contrato de trabajo, por escrito. El juez Wilkinson escribió en forma separada:

"Esta acusación no fue un intento de aplicar la ley de espionaje a la prensa, ya sea para la recepción o publicación de materiales clasificados."[516]

---

[514] Idem, p.128.
[515] Idem.
[516] Idem.

La casi inexistencia juicios contra periodistas bajo la Ley de Espionaje refleja una vacilación por parte del Ejecutivo para desplegarse contra la prensa. Una vacilación probablemente explicada al menos en parte por las distintas decisiones judiciales a propósito de la Primera Enmienda.[517] La única ocasión en que se ha invocado la Ley de Espionaje directamente contra la prensa no surgió en un proceso penal, sino que en el contexto de un intento de la Administración Nixon para obtener una orden judicial para impedir la publicación de lo que se conoce como los *"Pentagon Papers"*.[518]

III.3.2. A propósito de la Primera Enmienda.

III.3.2.1 Los "Pentagon Papers"[519](1971). Este es uno de los grandes casos de la Primera Enmienda y el que mejor proporciona un marco de estudio para un eventual *Assange v. United States*[520].

El gobierno presentó una solicitud de orden judicial contra la publicación de los documentos, basándose no sólo en su poder inherente para proteger la defensa nacional, sino que también invocó la sección 793 (e) de la Ley de Espionaje.[521]

El dilema no era si el periódico podría ser procesado criminalmente bajo la Ley de Espionaje, era si el gobierno tenía derecho a conseguir una orden de censura previa contra la publicación de información en nombre de la "seguridad nacional". La Corte, en una muy breve orden *per curium*, dictaminó que el gobierno no tenía el derecho solicitado.[522]

---

[517] Idem, p.129.
[518] Idem.
[519] *New York Times Co. v. United States.*
[520] El profesor Benkler coincide con ello. BENKLER, op. cit., p. 33.
[521] JONES, op. cit., p.129.
[522] Idem.

Fundamentó su decisión en la doctrina de la censura previa, declarando que "teniendo una fuerte presunción en contra de su validez", el gobierno cargaba con un pesado deber de justificación para tal restricción, dictaminando seis jueces contra tres que el gobierno no había "cumplido esa carga"[523].

La decisión del Tribunal Supremo fue una clara derrota para las alegaciones del gobierno vinculadas a la seguridad nacional y una victoria igualmente clara para la libertad de expresión y de prensa.[524]

Todos los jueces coincidieron en se requería actividad jurisdiccional, se debía analizar la colisión entre lo que los requirentes planteaban como tutela de la seguridad nacional y los valores y principios de la Primera Enmienda. Pero entre los jueces también hubo grandes diferencias de opinión sobre el alcance de la función jurisdiccional.[525]

III.3.2.1.a. La Primera Enmienda como absoluta: jueces Black, Brennan y Douglas. El único juez que tomó una posición categóricamente absoluta sobre la primera enmienda fue el juez Black, argumentando que:

"a cada momento la continuidad de las medidas cautelares en contra de estos periódicos constituye una violación flagrante, indefendible y continua de la Primera Enmienda",

sin darle cabida a las reclamaciones sobre la seguridad nacional[526], pues según él, estas reclamaciones tratan de justificar que:

"a pesar del enfático mandato de la Primera Enmienda, el poder ejecutivo, el congreso y el poder judicial puedan hacer leyes prohibiendo la publicación de noticias de actualidad y se coarte la libertad de prensa en nombre de la "seguridad nacional"[527].

[523] BARRON, op. cit., p.49, referencia 19.
[524] Idem, referencia n° 18.
[525] Idem, p. 50, referencia 26.
[526] Idem, referencia 27.
[527] Idem, p. 51, referencia 30.

Además, consideró que:

"la palabra "seguridad" es amplia, generalmente vaga, cuyos contornos no deben ser invocados para abrogar la ley fundamental consagrada en la Primera Enmienda"[528].

Consideró también que toda la seguridad que necesitaba el país ya era proporcionada por las garantías de la libertad de expresión y de prensa.[529] Finalmente invocando a Madison y a los demás autores de la Primera Enmienda, pensó que ellos la establecieron en un lenguaje que sinceramente creían nunca podría ser mal interpretado: "El Congreso no hará ninguna ley que coarte la libertad… de la prensa…" y que así, tanto la historia como el lenguaje de la Primera Enmienda apoyan la opinión de que la prensa debe quedar libre de publicar noticias, cualquiera que sea la fuente, sin censura, requerimientos o restricciones previas.[530]

Otro juez de posición parecida fue el juez Brennan, quien argumentó que:

"La Primera Enmienda se erige como un obstáculo absoluto a la imposición de restricciones judiciales en circunstancias como las que presentan estos casos"[531].

Objetó que la petición del gobierno de medidas cautelares se haya basado en la posibilidad de perjuicio al "interés nacional"[532]. Sin embargo, sólo había una justificación para una restricción previa y es que fuese durante la guerra[533]. La intervención militar estadounidense en Vietnam no fue precedida

[528] Idem, referencia 31.
[529] Idem, referencia 32.
[530] JONES, op. cit., p. 130 referencia 70.
[531] BARRON, op. cit., p.51, referencia 40.
[532] Idem, referencia 41.
[533] Idem, referencia 42.

de una declaración formal de guerra. Este fue el caso también de la Guerra del Golfo, la invasión de Irak, y el de la actual intervención militar en Afganistán[534].

Brennan no se refirió a la cuestión de la validez constitucional de la censura previa a la prensa durante las guerras no declaradas, sin embargo, hizo observar que, incluso en el caso de un holocausto nuclear, el ejecutivo:

"debe presentar necesariamente la base sobre la cual se busca la ayuda del control del poder judicial"[535].

Los tribunales se vieron obligados a exigir prueba. En los casos de la Primera Enmienda, los tribunales, no el ejecutivo, tendrían la última palabra[536].

La opinión del juez Douglas es igualmente categórica en relación a que la prensa no debe ser intervenida:

“no hay lugar para la restricción gubernamental sobre la prensa"[537].

Sin embargo, se diferenció en que sintió la necesidad de examinar la Ley de Espionaje para ver si había algún mérito en la posición del gobierno de que “la palabra “comunica” es lo suficientemente amplia como para abarcar la publicación”[538]. El concluyó que no[539]-[540]. Sin embargo, supongamos que serias consecuencias adversas fluían de la divulgación. Eso habría servido de base para la defensa de una censura previa en vistas del Juez Douglas, pero:

[534] Idem, referencia 43.
[535] Idem, p. 53, referencia 45.
[536] Idem, referencia 46.
[537] Idem, referencia 33.
[538] Idem, referencia 34.
[539] Idem, referencia 35.
[540] “Dado que ninguna ley autoriza la acción del poder ejecutivo, ninguna autoridad para aplicar una medida cautelar contra la prensa fluye de su "poder inherente". Tal poder puede existir si precedentemente existe una declaración de guerra del Congreso. Sin embargo, el Congreso no había emitido una declaración de guerra con respecto a Vietnam y las guerras presidenciales no estaban autorizadas. Por lo tanto, no había un caso de "poder inherente" tampoco.” Idem, referencia 38.

"El propósito dominante de la Primera Enmienda fue prohibir la práctica generalizada de la represión gubernamental de la información embarazosa"[541].

Para los jueces Black, Brennan y Douglas, la Primera Enmienda triunfó sobre consideraciones de seguridad nacional cuando el gobierno buscaba una medida cautelar contra la prensa. Sin embargo, para los otros tres magistrados que componían la mayoría - Stewart, Marshall y White - conciliar el conflicto de la seguridad nacional frente a la libertad de prensa era mucho más difícil de resolver[542] .

III.3.2.1.b. El tema del Estado de Derecho: jueces Stewart, White y Marshall. Para el juez Stewart en la era de la energía nuclear el presidente de los Estados Unidos tiene mayor "independencia constitucional" en las áreas de la defensa nacional y de las relaciones exteriores que un primer ministro de un país con un sistema parlamentario[543]. Pero, una opinión pública crítica, dependiente de una prensa "alerta, consciente y libre" sería el único freno real sobre las acciones del Presidente en estas áreas[544]-[545].

Piensa que las relaciones de defensa: "requieren tanto de la confidencialidad como del secreto"[546].

¿Cómo resolver el dilema entre la necesidad de confidencialidad por parte del gobierno y de la necesidad de libertad de prensa por parte de la gente? Para el juez Stewart la respuesta fue clara:

"La responsabilidad debe estar donde está el poder"[547].

¿Y donde está el poder?

---

[541] Idem, referencia 39.
[542] Idem, p. 53.
[543] Idem, referencia 47.
[544] Idem, referencia 48.
[545] También en BENKLER, op. cit, p. 34, referencia 202.
[546] BARRON, op. cit., p.53, referencia 49.
[547] Idem, referencia 50.

El ejecutivo debe resolver el dilema: esto es, el presidente debe: "determinar y preservar el grado de seguridad interna necesaria", para el ejercicio de sus responsabilidades en la defensa y asuntos exteriores[548].

El papel del Congreso en estas circunstancias es el de promulgar: "leyes penales específicas y apropiadas para proteger la propiedad del gobierno y preservar sus secretos"[549]. De hecho, el Congreso había aprobado leyes penales pertinentes a los hechos de este caso[550].

Si el gobierno decidió tramitar una orden de restricción preventiva en virtud de esta legislación vigente pertinente, entonces los tribunales tendrían que determinar si esta legislación era aplicable[551].

¿Qué estaba sugiriendo el juez Stewart? Que bajo la legislación vigente, la ley de espionaje, podrían presumiblemente establecerse cargos contra la editora del *Washington Post* y contra el editor del *The New York Times*. Pero por otra parte, el juez Stewart sostuvo que si el Congreso aprobara una ley que autorice, por ejemplo, al gobierno a prohibir la prensa en interés de la seguridad nacional, entonces los tribunales igualmente tendrán que determinar la aplicabilidad de los hechos del caso al estatuto hipotético, así como la constitucionalidad de una ley de este tipo.[552]

Dijo que el ejecutivo estaría en lo cierto respecto a que algunos de los Papeles del Pentágono deberían mantenerse en secreto "en el interés nacional"[553]. Pero luego hace un giro, diciendo que no podía afirmar que alguno de estos documentos podría causar daños irreparables a la nación[554]-[555]. Como

[548] Idem, referencia 51.
[549] Idem, p. 54, referencia 53.
[550] Idem, referencia 54.
[551] Idem, referencia 55.
[552] Idem, referencia 56.
[553] Idem, referencia 58.
[554] Idem, referencia 59. "Peligro de daño irreparable" era el estándar para otorgar la medida cautelar.

no había un daño irreparable, en virtud de la Primera Enmienda la única solución posible era la de negar la medida cautelar solicitada por el gobierno. Además, llega a la conclusión de que no corresponde que la resolución del conflicto entre la seguridad nacional y la libertad de prensa sea de competencia presidencial y que los tribunales se deban postergar.

La opinión del juez Marshall se enfoca desde la relevancia que le da al imperio de la ley. La cuestión fundamental para él fue determinar "si el Tribunal de Justicia o el Congreso tiene el poder de generar la ley"[556]. Para él estaba claro que la Constitución no permite a los tribunales o al poder ejecutivo crear una ley si el Congreso no lo ha hecho[557]. Marshall argumentó que esta no era una situación en la que el Congreso simplemente se haya olvidado de proporcionar un remedio a un grave problema[558]. Además, recordó que en el pasado, el Congreso había proporcionado al Ejecutivo "un amplio poder para proteger a la nación contra la divulgación de secretos de Estado perjudiciales"[559].

El juez Marshall señaló que la Ley de Espionaje establece que, si alguien tiene la posesión no autorizada de información perjudicial para Estados Unidos y esta "se comunica voluntariamente" a una persona que no tenga derecho a recibirla sería objeto de sanción penal[560]. Según esta interpretación, los editores del *Washington Post* y del *New York Times* podrían haber sido procesados, y de ser declarados culpables, multados o encarcelados, o ambas cosas. Admitió, sin embargo, que el significado de la palabra "comunica" en la ley no se refiere a "la publicación de artículos de prensa"[561]. A continuación,

---

[555] BENKLER, op. cit., p. 34, referencia 200.
[556] BARRON, op. cit., p. 55, referencia 61.
[557] Idem, referencia 62.
[558] Idem, referencia 63.
[559] Idem, referencia 64.
[560] Idem, referencia 65.
[561] Idem, referencia 66.

señaló diversas propuestas que se habían hecho al Congreso para hacer que "aquellas conductas fuesen ilegales" y que habrían dado "al Presidente el poder que busca en este caso"[562]. Sin embargo, reconoció que el Congreso se negó a aprobarlas[563].

La opinión del juez White hizo hincapié en un tema que el juez Stewart había tocado muy bien. De hecho, el Congreso había aprobado leyes penales pertinentes, señalando que la sección 798 de la Ley de Espionaje prohibía "conocer y publicar cualquier información clasificada concerniente a los servicios de sistemas criptográficos o actividades de comunicación de los servicios de inteligencia de Estados Unidos, así como cualquier información obtenida de las comunicaciones de operaciones de inteligencia"[564]. Lo que estaba diciendo era que la editora del *Washington Post*, y el editor del *New York Times* podrían ser procesados bajo esta disposición de la Ley de Espionaje. El juez White era bastante contundente aquí: "No tengo ninguna dificultad en sostener convicciones de que en estas secciones los hechos no justifican la intervención de la equidad y la imposición de una censura previa"[565]. Las raras excepciones a ello, requerirán una combinación de alta probabilidad, magnitud e inmediatez de daño para justificar la represión[566]. En el ámbito de la defensa nacional, esto es explicado por la frase "las fechas de salida de los transportes o el número y la ubicación de las tropas."[567]

Sin embargo, el gobierno había optado por no enjuiciar bajo la Ley de Espionaje. Ahora, la posición del gobierno era que los poderes constitucionales inherentes al Congreso y al Poder Judicial daban una base constitucional para

[562] Idem, referencia 67.
[563] Idem, referencia 68.
[564] Idem, p. 56, referencia 69.
[565] Idem, referencia 70.
[566] Ver la doctrina del test del peligro claro y presente a propósito de la doctrina de la censura previa en el párrafo pertinente al estudio sobre qué nos dice la Primera Enmienda, de este trabajo.
[567] BENKLER, op. cit., p. 34, referencia 204 a propósito del caso *Near vs. Minnesota*, 283 U.S. 697, 716 (1931).

emitir una orden judicial - una restricción cautelar - en contra de la prensa en estas circunstancias[568]. A diferencia del juez Black, el Juez White no dijo que la Primera Enmienda jamás permitiría "una orden judicial contra la publicación de información sobre los planes o las operaciones del gobierno"[569]. Sin embargo, llegó a la conclusión de que el gobierno no había cumplido con la:

"justificación excepcionalmente exigente bajo la Primera Enmienda"[570].

En resumen, para los jueces Stewart, Marshall, y White era de vital importancia que el Congreso no había aprobado una ley que autorizara interferir en la prensa. En este contexto, para ellos la Primera Enmienda no es absoluta, sino que la Corte no puede ni debe intervenir en ausencia de una ley que autorice a limitar a la prensa y, para el juez White, que tampoco se pudo establecer la existencia de un peligro claro y presente. Por lo tanto, en virtud de la Primera Enmienda, la única solución posible era la de negar la medida cautelar solicitada por el gobierno.[571]

Estos tres jueces aun siendo partes de la mayoría que determinó que el gobierno no tenía derecho a solicitar la orden previa, estimaron, sin embargo que el periódico podría ser procesado después del hecho.[572]

En efecto, el juez White señaló que:

"el fracaso del Gobierno para justificar las limitaciones anteriores no mide su derecho constitucional a una condena por la publicación criminal. (…) Que el Gobierno haya elegido erróneamente proceder por una orden judicial previa no significa que no podría proceder con éxito de otra forma".

[568] BARRON, op. cit., p. 56, referencia 71.
[569] Idem, referencia 72.
[570] Idem, referencia 73.
[571] Idem, p. 56.
[572] JONES, op. cit., p.130.

Como después no existió ningún intento por enjuiciar al periódico, los tribunales nunca fueron llamados a resolver la cuestión de si la Ley de Espionaje podría aplicarse a la prensa en aquella circunstancia.[573]

III.3.2.1.c. Votos de minoría: jueces Harlan, Blackmun y Burger: Harlan insistió en que la función jurisdiccional se ve limitada[574]. Esta conclusión la basa en la doctrina de la separación de poderes y en que el ejecutivo tiene "primacía constitucional en materia de relaciones exteriores"[575]. Sin embargo, reflexionó que de todas maneras los tribunales debían hacer dos cosas. En primer lugar, "determinar si el objeto de la controversia se encuentra o no dentro del ámbito de competencia del presidente en materia de relaciones exteriores"[576]. En segundo lugar, debe asegurársele al poder judicial por el jefe de departamento atingente que la seguridad nacional sufriría daños irreparables[577]. En el caso de los Papeles del Pentágono, la cabeza sería el Secretario de Estado o el Secretario de Defensa, debiendo presentarse personalmente a dar cuenta.

Por supuesto, esta revisión limitadísima sólo proporcionaría una ligera protección a los intereses de la Primera Enmienda. En realidad, según la concepción de Harlan, no habría necesidad de que el poder judicial examine realmente los documentos o datos en cuestión.

Si comparamos la opinión de Harlan con la de dos jueces de la mayoría - Stewart y White - observamos que ellos también habrían prestado mayor atención al ejecutivo si hubiese existido ley que autorizara una medida cautelar en contra de la publicación de información confidencial del gobierno. Sin embargo, es dudoso que hubieran limitado la función jurisdiccional a la medida

[573] Idem
[574] BARRON, op. cit., p.56, referencia 75.
[575] Idem, referencia 76.
[576] Idem, referencia 77.
[577] Idem, referencia 79.

establecida por el juez Harlan. Si la posición de este último hubiese prevalecido, la medida cautelar habría sido confirmada a pesar de la presunción de invalidez con que la Primera Enmienda mira tradicionalmente a las restricciones preventivas.[578]

El juez Blackmun dijo que sería importante analizar:

"el amplio derecho de la prensa de imprimir y. . . el limitado derecho del gobierno de prevenir"[579].

Estableció que después de estudiar el material, compartía las preocupaciones del gobierno de que la publicación de los documentos podría causar "la muerte de soldados, la destrucción de alianzas" y dificultar "negociaciones con nuestros enemigos"[580].

Resolvió que:

"la Primera Enmienda, después de todo, es sólo una parte de la Constitución entera"[581]. Finalizando con que no podía: "suscribirse a una doctrina del absolutismo ilimitado de la Primera Enmienda a costa de degradar otras disposiciones"[582].

Burger, Presidente del Tribunal Supremo, se quejó, al igual que los demás jueces de la minoría, que el caso llegó a los tribunales con indebida velocidad[583]. *The New York Times* tuvo posesión de los Papeles meses antes[584]. Los tribunales y el gobierno habrían estado obligados a hacer frente a los problemas de este caso dentro de un plazo de tiempo muy ajustado.

---

[578] Idem, p. 58.
[579] Idem, referencia 85.
[580] Idem, referencia 86.
[581] Idem, p. 59, referencia 87.
[582] Idem, referencia 88.
[583] Idem, referencia 91.
[584] Idem, referencia 92.

El juez Presidente consideró que el *Times* debió haber dado al gobierno la oportunidad de revisar los documentos[585]. Que debería haber tratado de llegar a un acuerdo con el gobierno sobre lo que debe y lo que no debe ser publicado. Dijo que, a pesar de estar en términos generales de acuerdo con los jueces Harlan y Blackmun, "no estaba dispuesto a llegar al fondo"[586].

El juez Burger, Presidente del Tribunal Supremo se unió al juez Blackmun en el razonamiento de que "la Primera Enmienda en sí misma no es un absoluto"[587]. Las opiniones de ambos omiten analizar detalladamente el papel del poder judicial en lo que respecta a las colisiones directas entre la primera enmienda y la seguridad nacional. Sin embargo, al menos implícitamente, hay un cierto desacuerdo entre Burger y Blackmun, por una parte, y Harlan por otra. Los primeros pensaron que los jueces deben revisar el material por sí mismos. Harlan, sin embargo, piensa que si a la Corte se le ha asegurado por el Ejecutivo que el tema de Seguridad Nacional es muy grave y requiere restricciones no es necesaria dicha revisión.[588]

En resumen, todos los jueces del caso Papeles del Pentágono piensan que debería haber alguna función judicial para decidir si el gobierno puede o no restringir la libertad de prensa en interés de la seguridad nacional. Sin embargo, hubo una gran diferencia de opinión sobre la naturaleza de ese papel.[589]

---

[585] Idem, referencia 93.
[586] Idem, referencia 94.
[587] Idem, referencia 95.
[588] Idem, p. 60.
[589] El juez Black entendía que era de la esencia misma de la función judicial el anular las acciones de restricción o cese contra la prensa obtenida por el gobierno. Para el juez Harlan, la función judicial era mucho más limitada. Si se involucraban las relaciones exteriores o la seguridad nacional, el poder judicial sólo debería extenderse a un mínimo de supervisión, aun cuando graves cuestiones de la primera enmienda se presenten. Los demás jueces se ubicaron en posiciones intermedias, algunos más cerca del absolutismo de la Primera Enmienda del juez Black, otros más cerca de las preocupaciones expresadas por el juez Harlan en cuanto a que la medida de control judicial debe ser permitida cuando el ejecutivo crea que la defensa o las relaciones exteriores de la nación son amenazadas. Idem, p. 60.

Alexander Bickel, abogado del *New York Times* en el caso, capturó las divergencias de opinión entre los jueces, cuando escribió: "Como yo concibo el concurso establecido para la Primera Enmienda, y como el Tribunal Supremo parece concebirlo en este caso, es que el deber que se presume en la prensa es el de publicar, no el de tutelar la seguridad o estar preocupado de la moralidad de sus fuentes"[590]

Al profesor Barron, le gustaría pensar que la afirmación anterior es lo que el caso de los Papeles del Pentágono representa. Sin embargo, como hemos analizado, de las opiniones de los jueces, parece que sólo cuatro de ellos: Black, Douglas, Brennan y Marshall han suscrito a aquella. Ciertamente, los disidentes - Harlan, Burger y Blackmun - no lo hicieron. Por otra parte, no estamos seguros de que Stewart y White se hayan adherido a esta declaración tampoco. Ellos, al igual que Marshall, estaban preocupados por la falta de autoridad legal. Sin embargo, la negativa del Congreso para promulgar una ley de ese tipo ni entonces ni ahora es una indicación de que la declaración de Bickel de que el "deber de la prensa es el de publicar, no el de proteger la seguridad"[591] reflejaría un entendimiento nacional sobre el significado de la Primera Enmienda.[592]

III.3.2.2. Caso AIPAC (2005)[593]. La aplicación de la Ley de Espionaje a personas que no tienen una posición de confianza con el gobierno, fuera del escenario de espionaje clásico (en el que un agente de un gobierno extranjero ofrece información perjudicial a tal gobierno hostil), ha sido motivo de controversia. Este es el único caso conocido de este tipo.[594]

---

[590] Idem, p. 61. referencia 101.
[591] Idem, referencia 102.
[592] Idem, referencia 103.
[593] También conocido como *United States vs. Rosen.*
[594] ELSEA, Jennifer K., *"Criminal prohibitions on the publication of classified defense information"*. [Prohibiciones penales relativas a la publicación de información clasificada de la defensa]. Congressional Research Service, 31 de enero de 2013, p. 17.

Siendo el paralelo más cercano al caso *WikiLeaks* en los últimos años, surgió cuando a dos empleados del grupo de *lobby "American Israel Public Affairs Committee"* (*"AIPAC"*) se les impusieron cargos por haber violado la Ley de Espionaje. No eran empleados del gobierno, sino que obtuvieron información sensible a través de una fuga de un empleado del Departamento de Defensa y luego la transmitieron o trataron transmitirla a otros.[595]

Steven J. Rosen sirvió durante 23 años como alto funcionario de *AIPAC*, mientras que Keith Weissman sirvió durante años como analista sobre Irán. Ambos fueron acusados en virtud de las secciones 793 (d)[596] y (g)[597] de la Ley de Espionaje en un complicado caso que se inició en 2005. Si el caso hubiese continuado hasta la etapa de prueba, hubiera sido la primera persecución bajo la Ley de Espionaje esencialmente sin documentos. En los procesamientos anteriores, los acusados habían transferido activos tangibles, como documentos o fotografías, a un gobierno extranjero. En este caso la información se transmite por vía oral.[598]

La acusación denunció que conspiraron para obtener información clasificada de funcionarios del gobierno con el fin de transmitirla a otros grupos de presión, periodistas y diplomáticos, incluidos los representantes de Israel. Parte de la información se refería a operaciones iraníes contra las fuerzas de EE.UU. en Irak. Lawrence Franklin, un funcionario que trabajaba en la oficina del secretario de Defensa, Donald Rumsfeld, pasó la información a Rosen y Weissman. Franklin se declaró culpable, entre otros cargos, por la comunicación y por la conspiración para transmitir la información de defensa a personas no autorizadas para recibirla. Fue condenado en enero de 2006 a poco más de doce años de prisión y a una multa de U$ 10.000. Su sentencia

[595] JONES, op. cit., p.133.
[596] Personas con posesión no autorizada de información de la defensa nacional que se transmiten a receptores no autorizados.
[597] Conspiración.
[598] JONES, op. cit, p.133.

fue posteriormente reducida a diez meses de arresto domiciliario por su cooperación en el caso *AIPAC*.[599]

Se procedió contra Rosen y Weissman por retransmitir a los miembros de la prensa y a otros la información supuestamente clasificada que habían recibido de Franklin. En respuesta, los acusados intentaron que se desestimase la acusación por varias razones, entre ellas, que la referencia de la ley a la "información relativa a la defensa nacional" era inconstitucionalmente vaga, que el estatuto violaba sus derechos de la Primera Enmienda y enfriaba los de los demás ciudadanos debido a la incertidumbre que se impondría sobre lo que de la discusión de asuntos de seguridad nacional estaría prohibido. Numerosos *amici curiae* presentaron escritos instando al tribunal de primera instancia desestimar los cargos por razones de libertad de expresión.[600]

En un dictamen de 2006, el Juez de Distrito T.S. Ellis negó la moción para desestimar la acusación, pues en su opinión la Ley de Espionaje era constitucional y aplicable a ambos procesados. Citando *US. vs Morison*, destacó que "la mera invocación de la "seguridad nacional" "o del "secreto de gobierno" no excluye un análisis de la Primera Enmienda.[601]

En primer lugar, revisando los casos *Gorin*, *Morison* y otros casos anteriores, el juez Ellis observó que el término "información relativa a la defensa nacional" se limita a la información "celosamente guardada" por el gobierno[602]. En segundo lugar, según el juez Ellis, los casos anteriores establecieron que la ley se aplica únicamente a la información del tipo cuya divulgación "sería potencialmente perjudicial para los Estados Unidos o útil para un enemigo de los Estados Unidos"[603]. En tercer lugar, la jurisprudencia también estableció que

[599] Idem.
[600] Idem.
[601] Idem.
[602] Idem, p. 134, referencia 90.
[603] Idem, referencia 91.

una condena en virtud de la ley obliga al gobierno a demostrar que el acusado "voluntariamente" violaba sus términos, es decir, actuaba específicamente para violarla[604]. Por último, cuando un proceso se basa en la invocación de "otra información relacionada con la defensa nacional", dando información intangible (en lugar de la difusión de documentos tangibles específicos, como un esquema de una base militar o un arma), sostuvo que la ley exige al gobierno demostrar que el acusado tuvo la intención subjetiva en la divulgación de la información "de dañar a Estados Unidos o ayudar a un gobierno extranjero."[605]

Ellis llegó a la conclusión de que estas limitaciones al alcance de la Ley de Espionaje que se aplican a un receptor civil de información de defensa nacional en forma intangible, reflejan una adecuada interpretación para que el gobierno proteja un interés de primer orden, como lo es, la seguridad de la nación, de manera que la ley sería consistente con la Primera Enmienda.[606]

En resumen, el juez Ellis articuló una imponente carga para el gobierno: Se tendría que probar que Rosen y Weissman actuaron con la intención de violar la ley, de difundir lo que sabían que era información secreta, que la información era objetivamente de un tipo tal que pudiese perjudicar a EE.UU., que Rosen y Weismann subjetivamente sabían del potencial de la información para dañar a EE.UU. cuando se haya publicado y que buscaban ese daño.[607]

A pesar de que pasaron casi tres años desde la fecha de esta sentencia, no fue una gran sorpresa cuando el 1° de mayo de 2009 los fiscales del caso anunciaron que pedirían el juez Ellis desestimar los cargos contra Rosen y Weissman, debido a "la disminución de la probabilidad de que el gobierno prevalezca en el juicio bajo los requisitos de intención adicionales impuestos por

[604] Idem, referencia 92.
[605] Idem, referencia 93.
[606] Idem, referencia 94.
[607] Idem, p. 134.

el tribunal y a la divulgación inevitable de la información clasificada que se produciría en la etapa de prueba".[608]

III.3.2.3. Bartnicki v. Vopper (2001). Un comentarista de radio recibe el correo de una fuente anónima con la grabación de una conversación telefónica interceptada ilegalmente, que el comentarista luego emite al aire. El Tribunal sostuvo que la emisión estaba protegida por la Primera Enmienda, a pesar de que la fuente anónima podría ser procesada por la comisión de una escucha telefónica ilegal. El Tribunal observó que la pregunta que se presentaba era si una persona que recibe información de una fuente que la ha obtenido de manera ilegal puede ser sancionada por difundir públicamente información relevante para el debate público, en ausencia de una necesidad de primer orden.

La Corte citó el caso de los Papeles del Pentágono resolviendo que no puede ser castigada la divulgación de información sobre la base de que había sido sustraída por un tercero. En circunstancias de ya estar disponible, la divulgación de la información por parte del beneficiario inocente estaría cubierta por la Primera Enmienda.[609]

La interpretación contemporánea de la Primera Enmienda parte de la premisa de que la libertad de expresión y de prensa garantizada por la Constitución comprende por lo menos la libertad de discutir públicamente y con la verdad todas las cuestiones de interés público y sin temor a un castigo subsiguiente.[610] En una serie de casos que comienzan con *Smith v. Daily Mail* en 1979, la Corte Suprema ha subrayado en repetidas ocasiones que "la

---

[608] Idem.
[609] ELSEA, op. cit, p. 26, referencia 165, citando a su vez *Boehner v. McDermott*, 484 F.3d 573 (*D.C. Cir*. 2007).
[610] JONES, op. cit., p. 140, referencia 119, citando a su vez a Lee Levine, Nathan E. Siegel and Jeanette Melendez Bead, *Handcuffing the Press: First Amendment Limitations on the Reach of Criminal Statutes as Applied to the Media*, 55 N.Y.L. SCH. L. REV. 1015, 1017 (2011) (quoting *Thornhill v. Alabama*, 310 U.S. 88, 101-02 (1940)).

información veraz sobre un asunto de interés público" recibe una muy amplia protección ante la responsabilidad penal o civil[611]. A menudo, llamado "el principio *Daily Mail*", este importante requisito constitucional fue explicado por el Tribunal Supremo en *Bartnicki v. Vopper*, un caso que surge bajo la Ley federal de escuchas telefónicas, la cual tipifica como delito la interceptación ilegal y difusión de las comunicaciones por cable e inalámbricas.[612]

Cuando se trata de información veraz sobre un asunto de importancia pública, la Corte reafirmó que "los funcionarios del Estado no pueden castigar constitucionalmente la publicación de la información, en ausencia de una necesidad de primer orden."[613]

De importancia para Assange, el Tribunal Supremo también hizo hincapié en que el grado de protección que ofrece la Primera Enmienda en este sentido no varía en base a la identidad del hablante o a la utilidad social percibida de la información difundida.[614]

Además, en *Bartnicki*, con referencia a la circunstancia de que el editor obtiene la información legalmente, pero sabe que la fuente de la misma ha actuado de manera ilegal en la obtención o difusión de ella, el Tribunal de Justicia declaró tajantemente que "la conducta ilegal de un extranjero no es suficiente para eliminar la protección de la Primera Enmienda a la expresión sobre un asunto de interés público"[615].

Cabe destacar que esta protección se rompe, la Corte ha dicho, cuando el editor va más allá de aceptar el material obtenido ilegalmente por otro, llegando a la participación real en la obtención ilegal del material.[616] Esto sin

[611] Idem, referencia 120, citando a su vez a *Smith v. Daily Mail*, 443 U.S. 97, 103 (1979).
[612] Idem, p. 140.
[613] Idem, referencia 121.
[614] Idem, p. 141.
[615] Idem, p. 141, referencia 124, citando a su vez a *Bartnicki*, 532 U.S. at 517-18, 528, 535.
[616] Idem, referencia 125.

duda explica las declaraciones en la propia *web* de *WikiLeaks* y en los sitios de las organizaciones que han lanzado modelos similares, de negar expresamente el deseo de inducir (y en algunos casos, de desconocer la voluntad de aceptar el fruto de) las revelaciones ilegales.[617]

III.3.2.4. Caso Jean v. Mass. State Police (2007). María T. Jean publicó en la Internet una grabación de audio y video de una detención sin orden judicial, a pesar de su conocimiento de que la grabación dada a ella se había hecho ilegalmente. [618]

Aplicando *Bartnicki*, el Tribunal de Apelaciones de EE.UU. para el Primer Circuito sostuvo que la Primera Enmienda protegía a Jean de responsabilidad criminal. El tribunal sostuvo que el interés del gobierno en la protección de las comunicaciones privadas, que fue "claramente implicado" en *Bartnicki*, era "prácticamente irrelevante" en este caso porque las comunicaciones interceptadas involucraron "una búsqueda por agentes de policía de la casa de un particular frente a ese individuo, su esposa, otros miembros de la familia, y al menos ocho agentes de la ley"[619]. El tribunal también sostuvo que el interés del Estado para castigar a un editor posterior de la información, podía incluso tener menos peso en este caso, donde se conocía la identidad del interceptor, y, presumiblemente, podría ser acusado y, de ser declarado culpable, castigado.[620]

Además, el tribunal determinó que no había distinción entre la "colaboración activa" en este último caso, con la conducta "pasiva" en *Bartnicki*. En ambos casos, el tribunal sostuvo, hubo una decisión de proceder con las

[617] Idem, p. 141.
[618] Idem.
[619] Idem.
[620] Idem.

revelaciones, aunque las cintas fueron obtenidas ilegalmente. Ambas revelaciones estaban protegidas por la Primera Enmienda.[621]

Recapitulando la jurisprudencia a propósito de la ley de espionaje, la importancia de *Gorin v. Estados Unidos (1941)* está en que nos establece los parámetros para reconocer el espionaje clásico; la de *Hartzel v. Estados Unidos (1944)* está en que en él la Corte Suprema de esbozó el estándar requisito de procesamiento de esta ley[622]; la de *Estados Unidos v. Morison (1988)* porque la Corte de Apelaciones de EE.UU. para el Cuarto Circuito examinó el alcance de la Ley de Espionaje en un contexto relacionado con la prensa. Morison, un empleado de la Inteligencia Naval envió fotografías clasificadas al editor jefe de una revista que resultaron publicadas, siendo condenado. Intentó ser calificado como fuente y argumentó que la ley no se le aplicaba porque no era un "espía clásico". La Corte rechazó este argumento, señalando que fue procesado por más delitos que el del espionaje clásico, y que la Ley se aplica correctamente a la divulgación de material clasificado a cualquier persona "que no tenga derecho a recibir" la misma. Además es relevante porque dos de los tres jueces que votaron por la condena lo distinguieron de la prensa, y en su conjunto la Corte señaló que, como empleado del gobierno, se le había puesto en su conocimiento el tenor de sus obligaciones en virtud de su contrato por escrito. Uno de los jueces aclaró que la acusación no fue un intento de aplicar la ley de espionaje a la prensa por recibir o publicar material clasificado, de hecho, la revista no fue perseguida.

Recapitulando la jurisprudencia a propósito de la Primera Enmienda, la importancia de los *"Pentagon Papers" (1971),* está en que siendo el caso que mejor proporciona un marco de estudio*,* fundamentó su decisión en la doctrina

[621] Idem, p. 142.
[622] "[s]alvo que encuentren pruebas suficientes de que un jurado pudiese inferir más allá de una duda razonable de que tenía la intención de llevar a cabo las consecuencias específicas prohibidas por la ley, un ciudadano estadounidense tiene derecho a discutir estos temas, ya sea por medio de la razón templada o la inmoderación despiadada, sin violar la Ley de Espionaje de 1917".

de la censura previa, dictaminando seis jueces contra tres que el gobierno no tenía derecho a conseguir una medida prejudicial de censura pues no había cumplido la carga de sobrepasar una pesada presunción de invalidez de la solicitud. Tres jueces entendieron la Primera Enmienda como absoluta, considerando el más categórico de ellos que "la palabra "seguridad" es amplia, vaga, cuyos contornos no deben ser invocados para abrogar la ley fundamental consagrada en la Primera Enmienda", considerando también que la seguridad necesaría para el país ya la proporcionaba la libertad de expresión. Sin embargo, para los otros tres magistrados de la mayoría conciliar el conflicto de la seguridad nacional frente a la libertad de prensa era mucho más difícil de resolver. Para ellos fue vital que el Congreso no haya aprobado una ley que autorizara interferir en la prensa. Para ellos, la Corte no puede ni debe intervenir en ausencia de una ley que autorice a limitar a la prensa; A su vez, la importancia del caso *AIPAC (2005)* se radica en que el juez articuló una imponente carga para la operatividad de la ley de espionaje. Se tendrá que probar que se actuó con la intención de violar la ley, de difundir lo que sabía que era información secreta, que la información era objetivamente de un tipo tal que pudiese perjudicar a EE.UU., que subjetivamente se sabía del potencial de la información para dañar a EE.UU. cuando se haya publicado y que se busca provocar ese daño; La importancia de *Bartnicki v. Vopper (2001)* está dada en que se resolvió que no puede ser castigada la divulgación de información sobre la base de que había sido sustraída por un tercero. Encontrándose ya disponible, la divulgación de la información por parte del beneficiario inocente estaría protegida, haciéndose hincapié en que el grado de protección no varía en base a la identidad del hablante o a la utilidad social percibida de la información difundida; la importancia de *Jean v. Mass. State Police (2007)* está en que sostuvo que el interés del Estado para castigar a un editor posterior podía incluso tener menos interés pues se conocía al interceptor, y que no

había distinción entre la "colaboración activa" en este último caso, con la conducta "pasiva", ambas protegidas.

III.4. ¿QUE PREGUNTAS SE HA HECHO LA DOCTRINA?

De importancia fundamental para dilucidar este caso será exponer las preguntas que se han hecho los principales profesores y expertos en libertad de expresión y tecnologías, su argumentación y la fundamentación de sus respuestas, dando cuenta también de la riqueza de los argumentos.

Los informes de prensa indican que el Departamento de Justicia ha considerado cargos asociados más específicamente ya sea con la Ley de Espionaje ya sea con la Ley de Fraude y Abuso Informático.[623]

III.4.1. ¿Se podría procesar a Julian Assange según la ley de Fraude Informático?

Antes de dar respuesta a la pregunta es de interés en el ámbito del ciberderecho distinguir tres tipos de conductas según la intensidad de su potencial daño. Hablamos, en orden decreciente, de ciberterrorismo, hacking y ciberactivismo y comenzar a dilucidad si corresponden con los actos realizados por Julian Assange.

III.4.1.1. ¿Los actos de WikiLeaks son ciberterrorismo?

III.4.1.1.a. ¿Qué es el ciberterrorismo? Existen muchas malas interpretaciones en la definición de terrorismo cibernético, el término se estructura de la reunión de la cotidiana palabra "ciber" y de la menos cotidiana

[623] BENKLER, op. cit, p. 42, referencia 252 citando al The New York Times, Charlie Savage, *Building A Case for Conspiracy by Wikileaks*, 16 de diciembre de 2010, [en línea] http://query.nytimes.com/gst/fullpage.html?res=9B0DE2DF123CF935A25751C1A9669D8B63&ref=charliesavage. [Consulta: 07/07/2013].

"terrorismo". Mientras "ciber" es todo lo relacionado con nuestra herramienta de trabajo, el "terrorismo", por naturaleza es difícil de definir. Incluso el gobierno de EE.UU. no ha podido ponerse de acuerdo sobre una definición.[624]

La ambigüedad en la conceptualización implica la indistinción de lo que constituye la acción, como D. Denning señaló en su obra[625], una bomba de correos electrónicos podría ser considerada por algunos *hacktivismo* y por otros ciberterrorismo.

De ello se desprende que existe un grado de incomprensión con el significado de ciberterrorismo, ya sea desde los medios de comunicación, desde fuentes secundarias, o desde la experiencia personal. Incluso los especialistas utilizan diferentes conceptos. Barry Collin, que en 1997 se atribuyó la creación del término, lo define como:

"la convergencia entre la cibernética y el terrorismo"[626].

El mismo año, Marcos Pollitt, agente especial del *FBI*, ofrece la suya:

"es el premeditado ataque con motivaciones políticas contra los sistemas de información, informática, programas informáticos y sus datos, haciendo

[624] KRASAVIN, Serge. *"What is Cyber-terrorism?"*. [¿Qué es el ciberterrorismo?]. SANS Institute, July 2000, [en línea] < http://www.crime-research.org/library/Cyber-terrorism.htm> [Consulta: 02/09/2013]
"En el *Terrorism research center* http://www.terrorism.com/ se expone la definición del FBI: "El terrorismo es el uso ilegal de la fuerza o la violencia contra personas o propiedades para intimidar o coaccionar a un gobierno, la población civil o cualquier segmento de la misma, en cumplimiento de sus objetivos políticos o sociales". Por su parte la definición del Departamento de Estado es: "violencia premeditada, políticamente motivada perpetrada contra objetivos no combatientes por grupos subnacionales o agentes clandestinos. (20/07/2000)". Referencia 3.

[625] DENNING, Dorothy E. *"Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy"*. [Activismo, Hacktivismo y Ciberterrorismo: La Internet como herramienta para influir en la política exterior]. [en línea] <http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf> [Consulta: 02/09/2013]

[626] Krasavin, op. cit., referencia 5, citando a su vez a Barry Collin, *"The Future of CyberTerrorism"*, Proceedings of 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago, 1996.

posible la violencia contra objetivos no combatientes por grupos subnacionales o agentes clandestinos"[627].

La reconocida experta Dorothy Denning define el ciberterrorismo como:

"ataques ilegales y amenazas de ataques contra los computadores, las redes y la información en ellos almacenadas cuando se hace para intimidar o coaccionar a un gobierno o su pueblo en apoyo de los objetivos políticos o sociales"[628] .

Rod Stark lo define como: "cualquier ataque contra una función de información, independientemente de los medios"[629]

Las conceptualizaciones antes mencionadas incluirían cualquier ataque contra las telecomunicaciones, incluso la desfiguración de sitio y otras bromas informáticas en el concepto de ciberterrorismo.[630]

Sin embargo otro experto, James Christy, del *Defense-wide Information Assurance Program*, dirigido por la subsecretaría de Defensa para la dirección, control, comunicaciones e inteligencia, afirma que nunca una acción de ciberterrorismo ha sido emprendida contra los Estados Unidos. "Por el contrario, los eventos de *hacking* - incluyendo una página *web* de 1998 creada por partidarios del grupo mexicano de rebeldes zapatistas, que condujo a los ataques contra militares estadounidenses de 1.500 posiciones en 50 países distintos - constituyen delitos informáticos[631]. William Church, un ex oficial de Inteligencia del Ejército de EE.UU., quien fundó el *Center for Infrastructural*

[627] Idem, referencia 6, citando a su vez a Mark M. Pollitt. *"A Cyberterrorism Fact or Fancy?"*, Proceedings of the 20th National Information Systems Security Conference, 1997, pp. 285-289.
[628] DENNING, Dorothy E. *"CYBERTERRORISM"*. [CIBERTERRORISMO]. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives by Georgetown University, May 23, 2000, [en línea] <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html> [Consulta: 02/09/2013]
[629] Krasavin, referencia 11 citando a su vez a Rod Stark. *"Cyber Terrorism: Rethinking New Technology"*. Department of Defense & Strategic Studies Graduate Assistant Southwest Missouri State University, [en línea] <http://www.infowar.com/mil_c4i/stark/Cyber_Terrorism-Rethinking_New_Technology1.html> [Consulta: 02/09/2013]
[630] Idem.
[631] Idem, referencia 12, citando a su vez a Catherine MacRae. *"Cybercrime Vs Cyber Terrorism, DOD Official Says U.S. Has Been Victim Of Cyber Crimes, Not Terrorism"*. Defense Information and Electronics Report, 10/01/99.

Warfare Studies, está de acuerdo en que Estados Unidos no ha visto una amenaza terrorista cibernética en los terroristas que utilizan técnicas de guerra de información: "Ninguno de los grupos que se definen convencionalmente como grupos terroristas han utilizado armas informáticas contra la infraestructura"[632]. Richard Clarke, coordinador nacional de seguridad, protección de infraestructura y contraterrorismo en el consejo de seguridad nacional, ofrece dejar de usar el término "ciberterrorismo" y en su lugar utilizar el de "guerra informática".[633]

Las observaciones mencionadas generan una línea clara entre el ciberterrorismo y la delincuencia cibernética. Aun no hemos sido testigos de un ciberataque que haya causado grandes destrozos o pérdidas humanas, es decir, que nos induzca a proclamar el inicio de una verdadera ciberguerra o un ataque ciberterrorista, ya que hasta el momento, sólo se han encontrado rastros de visitas o intentos de acceso a infraestructuras estratégicas, pero sin mayores consecuencias.[634]

Los ataques se han limitado a colapsar los servicios de sitios *web* de instituciones o empresas, como en su caso más representativo en Estonia en 2007[635], inutilizar sistemas de comunicación, como en la Guerra del Golfo, 1991 o contrainformar como en la Guerra de Kosovo, 1999.

---

[632] Idem, referencia 13, citando a su vez a John Borland. "*Analyzing The Threat Of Cyberterrorism"*. TechWeb News, [en línea] <http://repository.binus.ac.id/content/M0104/M010417919.pdf>, [Consulta: 02/09/2013]

[633] Idem, referencia 14, citando a su vez, Dan Verton. *"Are cyberterrorists for real?"*, [en línea] < <http://edition.cnn.com/2000/TECH/computing/07/03/real.cyberterror.idg/> (07.03.00), [Consulta: 02/09/2013]

[634] SANCHEZ, Gema. *"Cibercrimen, ciberterrorismo y ciberguerra: Los nuevos desafíos del s. XXI"*, Revista Cenipec, 31, 2012, p.247.

[635] Constantes disputas hubo entre Rusia y Estonia. La OTAN se preocupó suficientemente como para enviar a expertos en ciberterrorismo a la capital de Estonia para investigar una importante denegación de servicio que duró tres semanas, atacando sitios *web* de su administración pública y de sus empresas privadas, así como las redes de telefonía celular del país.

Finalmente, nosotros definimos ciberterrorismo como: “ataques ilegales contra los computadores, las redes y la información en ellos almacenadas que hayan causado grandes destrozos o pérdidas humanas, cuando se hacen para intimidar o coaccionar a un gobierno o su pueblo en apoyo a sus objetivos políticos o sociales”.

III.4.1.2. ¿Los actos de WikiLeaks son hacking o es posible que sean hacktivismo?:

III.4.1.2.a. ¿Qué es el hacking? En un principio en las décadas de los ´50 y ´60, *“hack”* era una palabra de jerga utilizada por primera vez por los estudiantes del Instituto de Tecnología de Massachusetts, *MIT,* para referirse a '”una broma inteligente, benigna y ética o una broma pesada, a la vez un desafío para los autores y divertida para la comunidad *MIT*”.[636]

Estonia decía que los ataques se habían originado en Rusia. La UE y la OTAN han tenido cuidado de no acusar a Moscú, y el embajador de Rusia en Bruselas dijo a *The Guardian* en Gran Bretaña que una acusación a su país sería grave y “tendría que ser fundada”.
Estonia provocó la ira de Moscú el 27 de abril. La estatua de bronce de un soldado ruso indica la presencia de las tumbas de los rusos que murieron luchando contra el nazismo. Estonia trasladó la estatua, así como los restos de un cementerio militar lejos del centro de la ciudad argumentando que atraía fanáticos. Rusia acusó a Estonia de tratar de revisar la historia de la Segunda Guerra Mundial, buscando honrar más a los nacionalistas estonios que habían colaborado con los nazis más que a aquellos que cooperaron con los soviéticos. Los ánimos se caldearon en Estonia, hubo disturbios y saqueos en Tallin y entre estonios de origen ruso mataron a una persona e hirieron a otras 150.
Los ataques cibernéticos comenzaron después de los disturbios. Llegaron en oleadas, llegando a su máximo alrededor de las fechas significativas del 8 y 9 de mayo (el día de la victoria, una importante fiesta en Rusia). Los *hackers* organizaron ataques distribuidos de denegación de servicio desde computadores de todo el mundo. Funcionarios estonios afirmaron que algunos ataques eran rastreables llegando su huella hasta las instituciones del Kremlin. “Estos ataques provenientes de direcciones *IP* oficiales de autoridades rusas no sólo se dirigen contra nuestros sitios *web*, sino que contra nuestra cobertura para teléfonos móviles y nuestra red de servicios de rescate, lo que ya es muy peligroso”, dijo el ministro de Relaciones Exteriores de Estonia, Urmas Paet, al *The Times* de Londres. “Pueden costar vidas. Esperamos detenerlos, pero los ataques continúan.”
El portavoz del *Kremlin* Dmitry Peskov dijo a la *BBC* que las acusaciones eran “completamente falsas”.
Un funcionario de la OTAN no identificado dijo a *The Guardian*: “No voy a señalar con el dedo. Pero no se trataba de cosas hechas por unos pocos individuos… claramente hubo una organización”. DER SPIEGEL, *“Old Wars and New: Estonians Accuse Kremlin of Cyberwarfare”*, 17 de mayo de 2007, [en línea] <http://www.spiegel.de/international/world/old-wars-and-new-estonians-accuse-kremlin-of-cyberwarfare-a-483394.html> [Consulta: 02/09/2013]

[636] MCQUADE, Samuel, *“Encyclopedia of cybercrime”*, Greenwood Publishing Group, 2009, p. 87.

En el ambiente del *MIT*, con una combinación entre la tecnología disponible, estudiantes ambiciosos y desprecio general por las medidas de seguridad, se produjo lo que hasta hoy conocemos como "ética *hacker*". Explicada por Steven Levy en su libro *"Hackers: Heroes of the Computer Revolution"* de 1984 constaba de los siguientes seis principios fundamentales:

Primero, el acceso a los computadores y cualquier cosa que pueda enseñarte algo acerca de como la tecnología funciona en el mundo debe ser ilimitado y total; Segundo, toda la información debe ser libre y abierta; Tercero, desconfía de la autoridad, promueve la descentralización; Cuarto, los *hackers* deben ser juzgados por su *hacking*, no por criterios falsos como títulos, edad, raza o posición; Quinto, se puede crear arte y belleza desde un computador; y Sexto, los computadores pueden cambiar tu vida para mejor.[637]

Las personas que inicialmente se consideraban *hackers* tenían actitudes creativas y bromistas hacia la computación, pero a medida que las tecnologías informáticas y de redes se han hecho más avanzadas y accesibles, muchos nuevos usuarios de computadores asumieron la etiqueta de *hacker* y comenzaron a utilizar la ética *hacker* para justificar actividades criminales. Los medios de comunicación, a su vez, comenzaron a informar sobre las nuevas formas de delitos informáticos cometidos por estas personas, dando lugar a la creencia general del público de que todas las actividades llamadas *hacking* eran ilegales, siendo una fuente común de confusión incluso hoy. Mientras los medios de comunicación empujaban la etiqueta *hacker* más lejos de la ética del *hacker* original, el aspecto comunitario del *hacking* se mantuvo.[638]

Los *hackers* delincuentes se unieron para formar grupos de *hackers* en línea a través del sistema *Internet Relay Chat*, *IRC*. Sin embargo, un reciente aumento en el número de personas dedicadas a diversas formas de

[637] Idem.
[638] Idem, p. 88.

modificaciones de *hardware* ha comenzado a cambiar la definición popular de *'"hacker"* de nuevo hacia la definición original, no criminal, esta vez presionando por modificaciones legales.[639]

Hoy en día, las personas que se describen como *hackers* son un grupo diverso, que incluye tanto aquellos que se suscriben a la ética *hacker* original y quienes se dedican a actividades delictivas. En su conjunto, este grupo de personas representa una subcultura *hacker* que hoy en día incluye sitios *web*, publicaciones y congresos que reúnen a miles de personas en todo el mundo.[640]

Así, la conceptualización del término *"hacking"* ha variado a lo largo de las décadas permaneciendo hasta el día de hoy como un concepto con una cara positiva y otra negativa. Naturalmente, habiendo llegado este concepto a sede legislativa penal, esencialmente se ha referido a los: "actos de acceso no autorizado a los sistemas de información, incluyendo las redes de computadores". Según se define en las leyes sobre delitos informáticos estatales y federales de los Estados Unidos, ello se extiende a las personas que extralimiten sus permisos autorizados dentro de una red informática determinada.[641]

III.4.1.2.b. ¿Qué es el hacktivismo? Se ha definido como la utilización con fines políticos no violentos de "herramientas digitales ilegales o legalmente ambiguas" como *desfiguraciones web*[642], robo de información[643], parodias de

[639] Idem.
[640] Idem.
[641] Idem, p. 87
[642] Es considerada la forma más común de *hacktivismo*, consiste en obtener acceso no autorizado a un servidor *web* y, o bien sustituir o modificar la página *web* con nuevos contenidos transmitiendo un mensaje particular, pudiendo estar limitada a un solo sitio, o reproduciéndolo en grandes volúmenes a través de cientos o miles de sitios, con el fin de comunicar un mensaje relacionado a una causa y de demostrar la destreza técnica del desfigurador. HAMPSON, op. cit., p. 519 – 520.

sitios *web*, ataques *DoS*[644], *site redirects*[645], *sit-in* virtuales[646] y el sabotaje virtual.

Su historia comienza contemporáneamente a la de Internet teniendo sus orígenes en el *hacking* y el activismo, por lo que distinguirlo del *hacking* no es sencillo. En cierto sentido, tienen motivos divergentes: el *hacking* se hace a menudo por propio interés de los *hackers*, mientras que el *hacktivismo* se hace a menudo para conseguir un objetivo social o político. Además, el *hacking* se practica con frecuencia en la defensa o promoción de un conjunto único de normas que se han desarrollado como parte de la cultura de la Internet. Para nuestros propósitos, sin embargo, el *hacking* puede distinguirse del *hacktivismo*, en que aquel carece de objetivos políticos.[647]

---

[643] Posiblemente indistinguible del robo ordinario, implica el acceso no autorizado a un ordenador o a una red y el robo de datos privados. A pesar de su ilegalidad, es sorprendente y penosamente bien aceptada por los *hacktivistas.* Idem. p. 520.

[644] Fue una forma de *hacktivismo* utilizada frecuentemente durante el incidente *WikiLeaks* y consiste en intentos de bloquear el acceso a sitios *web* por cualquiera de varios medios. Se busca que el acceso al sitio objetivo se ralentice significativamente o simplemente no se logre mientras el ataque está en marcha. Durante un tipo común de ataque *DoS*, la parte que lo inicia satura el servidor de la computadora que aloja el sitio *web* de destino con solicitudes de información, aumentando dramáticamente su consumo de recursos computacionales logrando hacer que el servidor sea más lento o se "resetee".
Una iteración popular del ataque *DoS* es un ataque *DDoS*, que se puede distinguir de un ataque DoS por el uso de una red de múltiples computadores atacantes. En un ataque *DDoS*, la parte que ataca activa una red de ordenadores bajo su control, denominada *botnet*, para multiplicar la potencia del ataque, dirigiendo de ese modo en forma exponencial un aumento del volumen de solicitudes de información al servidor de destino. Debido a la estructura de la Internet, los ataques *DDoS* a menudo implican las leyes de varios países. Una parte que inicialmente se encuentra en el país A puede controlar una red de computadoras ubicadas en los países B, C y D para atacar un sitio *web* alojado en servidores ubicados en el país E. "De este modo, la víctima, las pruebas y el autor pueden estar ubicados en diferentes países, muchos de los cuales probablemente tienen diferentes regímenes de seguridad cibernética, o ningún régimen en absoluto. Idem, p. 518.

[645] Como el nombre sugiere, dirige a los usuarios a un sitio diferente al que indica la dirección *web*. Es decir, mediante la obtención de acceso no autorizado a un servidor *web* y el ajuste de los parámetros de la dirección, logra que los usuarios lleguen a un sitio alternativo siendo este muy a menudo crítico de la página e destino original. Idem, p. 520.

[646] Se puede asimilar a un ataque DDoS en el sentido de que el objeto de los dos métodos es ralentizar o colgar al servidor objetivo abrumándolo con solicitudes de información. La diferencia está en que en lugar de comandar una red *botnet*, implican manifestantes individuales que atoran las páginas *web*, sea sólo manualmente volviendo a cargar varias veces la página *web* específica o permitiendo a los participantes descargar un código especial que automáticamente vuelve a cargar la página. Se la considera una forma masiva y democrática de *hacktivismo*. Idem.

[647] Idem, p. 516.

Muchas formas de *hacktivismo* explotan el acceso ilegal a las redes con fines de lucro, y causan daños costosos. Métodos como las redirecciones *web*, los ataques *DDoS*, el robo de información y los sabotajes virtuales cuentan como acciones cuyos principales componentes podrían ser parte de un procedimiento penal. Estas formas de *hacktivismo* podrán llevarse a cabo con el fin de expresar algún mensaje, pero los medios utilizados implicarían renunciar a solicitudes de protección.[648]- [649]

Otras formas se utilizan principalmente para promover el cambio político o social. La ley vigente en los países más desarrollados, entre ellos Estados Unidos y el Reino Unido, en general prohíben el *hacktivismo*. Sin embargo, estos países también protegen el derecho a la protesta como un elemento esencial de la libertad de expresión. Las formas de *hacktivismo* que son principalmente expresivas, que no causan grave daño y que no explotan el acceso ilegal a las computadoras o redes, se asemejan suficientemente a las formas tradicionales de protesta como para garantizarles protección ante la aplicación de las leyes contra el *hacking* en coherencia con los principios de la libertad de expresión.[650]

En un intento de coordinar los esfuerzos contra el *hacking* internacional, el Consejo de Europa generó en 2001 la Convención sobre la ciberdelincuencia estableciendo un marco para los regímenes jurídicos nacionales. Los regímenes prescritos tienen un alcance general, y posiblemente podrían aplicarse a expresiones de *hacktivismo* que se asemejan a las formas tradicionales de protesta. El sistema jurídico de Estados Unidos cuenta con principios y doctrinas de protección a la libertad de expresión, y entendiéndose el *hacktivismo* como una forma de protesta como las desde antiguo

[648] Idem, p. 538.
[649] Las formas de *hacktivismo* que causan importantes daños financieros resultado del robo de información o daños en los servidores ocasionados por la instalación de un *malware*, deben ser diferenciados de *hacktivismo*, y se les prohíbe correctamente concibiéndose como ciberdelincuencia. Idem, p. 539.
[650] HAMPSON, op. cit., p. 511.

establecidas, estas doctrinas se podrían utilizar para proteger un subconjunto limitado de *hacktivismo*.[651]

En el contexto de la Primera Enmienda, las contribuciones al debate ciudadano sobre cuestiones de interés público se consideran esenciales para una democracia que funciona, y la Corte Suprema ha sido muy reacia a permitir el castigo de las declaraciones en este plano.[652]-[653]

No se sigue, sin embargo, que si algún daño es causado por un acto de *hacktivismo*, el acto deba ser considerado criminal. Puede ser que algunas formas de *hacktivismo* admisibles, como *sit - ins* y voluntarios ataques virtuales *DDoS*, no imponen un costo en los objetivos de la protesta. En un ejemplo reciente relacionado con *WikiLeaks*, un masivo ataque *DDoS* contra un *blog* en *WordPress.com* trajo como resultado problemas de conectividad para otros usuarios de *WordPress*. En otro ejemplo, los ataques *DDoS* a *Twitter* en 2009 hicieron que el sitio cerrara durante varias horas, y que varias de las características del servicio permanecieran no utilizables por algunos momentos. Aunque estos ataques fueron aparentemente dirigidos a usuarios individuales de ambos servicios, sus efectos tuvieron implicaciones para millones de otros usuarios. Los servicios probablemente dedicaron mucho tiempo y recursos a la

[651] Idem, p. 521.

[652] Incluso las protestas que irriten al público o causen emociones potencialmente perjudiciales para la paz cívica estarán protegidas siempre y cuando no estén "dirigidas a incitar o producir acciones delictivas inminentes y [no sean] susceptibles de incitar o producir tales acciones." Idem, p. 526 – 527.

[653] La facultad del gobierno para limitar la protesta a través de la imposición de un plazo razonable, de la determinación de un lugar y las restricciones a las formas de la libertad de expresión, sin embargo, son en gran parte no cuestionadas. En este sentido, las protestas se pueden canalizar, pero no ser sofocadas por completo, si son pacíficas y se refieren a cuestiones de interés público.
Este tipo de restricciones deben ser "de contenido neutral", no se puede prohibir el discurso justificándose en el tema de que trata, la identidad o punto de vista del orador, deben servir a un interés gubernamental importante y se deben dejar abiertas amplias vías alternativas para la comunicación. Tales restricciones son permisibles, incluso en el discurso que se produce en lugares como las calles públicas, que tradicionalmente se han utilizado para el intercambio de ideas. En el contexto de la Internet, y tal como se aplica específicamente al *hacktivismo*, no está del todo claro plazo de restricción sería permisible, ni tampoco de lugar y forma. Idem, p. 527

defensa y recuperación de los ataques. Estos solos hechos lamentables, sin embargo, no justifican la tipificación penal de los ataques.[654]

Las protestas y manifestaciones causan molestias, irritación y distracción, pudiendo obstaculizar el comercio. El objetivo de una forma admisible de ciberprotesta debe tolerar las molestias causadas por el *hacktivismo*. Es parte del precio a pagar por la libertad de expresión.[655]

El resultado es que las organizaciones y los gobiernos que antes estaban aislados de la crítica en virtud de la censura, la opresión o la distancia física ahora son presa fácil. En los países que restringen el acceso a Internet, no residentes motivados pueden dar voz a la disidencia que de otra manera no hubiese sido escuchada. Y donde las protestas callejeras están sujetas a represión, el *hacktivismo* es un medio razonablemente seguro de manifestarse contra un régimen, pudiendo también ser una herramienta útil para la comunicación de las quejas contra las empresas, como lo demostró *Anonymous* con sus ataques durante el episodio *WikiLeaks*.[656]

A propósito de las empresas multinacionales, el *hacktivismo* puede permitir que las personas se quejen contra las empresas, aunque la sede central se encuentre en otro continente. En otras palabras, el *hacktivismo* se ofrece como un instrumento mediante el cual el objeto de la protesta no puede evitar ser blanco en virtud de su poder, de su ubicación, o por la pobreza o la opresión de las personas.[657]

III.4.1.3. ¿El gobierno podría utilizar la ley de Fraude Informático con probabilidades de éxito?

[654] Idem, p. 539 – 540.
[655] Idem, p. 540.
[656] Idem, p. 541.
[657] Idem, p. 542.

Si bien esta ley a primera vista parece ser la más atingente para ser invocada, la doctrina la ha entendido aplicable sólo contra Manning[658], que al "excederse en el acceso autorizado" a las computadoras del gobierno, "comunica voluntariamente" información clasificada que "se podría utilizar para la lesión de los Estados Unidos, o en beneficio de cualquier nación extranjera" a "una persona no autorizada para recibirla."[659]

De hecho, en el único supuesto en que Assange podría ser procesado según esta ley, es en el supuesto de que haya *hackeado* equipos del gobierno. Sabida la cooperación determinante de Manning en allegar los antecedentes a Assange y las posibilidades que habría otorgado la red de servidores voluntarios Tor, la posibilidad parece alejarse.

Pero de establecerse el poco practicable escenario de comprobar esa conducta, aun la posibilidad de procesamiento y condena sería desde controvertida a improbable, existiendo incluso el precedente de que la Corte estatal de Kansas decretó la nulidad del concepto esencial de esta ley, esto es, del concepto de "acceso" fundamentalmente debido a su vaguedad[660]. Por lo que en el caso de presentarse una acusación según esta ley ante la Corte Suprema podría inclusive aducirse la inconstitucionalidad de esta ley o por lo menos de este concepto y hacer caer el requerimiento.

III.4.2. ¿Se podría procesar a Julian Assange según la ley de Espionaje?

[658] BENKLER, op. cit., p. 43.
[659] 18 U.S.C. §1030 (a)(1).
[660] En *State vs. Allen (1996)* la Corte Suprema de Kansas sostuvo que su concepto era nulo debido a su vaguedad. CLOUGH, op cit, p. 155.

La opción más sugerida por la doctrina es que la acusación seguramente se tramitaría bajo la *Espionage Act*. Como vimos en el caso Papeles del Pentágono, varios jueces consideraron que era posible un proceso penal contra los editores de los periódicos a pesar de que no podían apoyar la solicitud del gobierno de una medida cautelar contra la publicación ante la ausencia de una ley[661]. Se tomó esta posición porque creían que la ley de Espionaje podría haber apoyado un proceso penal. Sin embargo, la doctrina cuestiona si la ley de Espionaje podría ser utilizada con éxito contra Assange[662].

III.4.2.1. ¿Podría EE.UU. alegar que la Ley de Espionaje extiende su ámbito de aplicación a conductas fuera de Estados Unidos, realizadas por ciudadanos no estadounidenses, y que la protección de la Primera Enmienda no se les aplica?

Acerca de su aplicabilidad en el extranjero, La Ley de Espionaje no da ninguna indicación expresa de que se pretenda aplicar extraterritorialmente, aunque los tribunales no han sido renuentes a aplicarla a la conducta de los estadounidenses en el extranjero[663].

Pero ello no responde a la cuestión de si el acto está destinado a aplicarse fuera de los Estados Unidos a ciudadanos no estadounidenses. Porque el espionaje es reconocido como una forma de traición a la patria, que generalmente se aplica sólo a las personas que le deben lealtad a los Estados Unidos, pudiéndose suponer que el Congreso no lo considera como un delito que pueda ser cometido por un extranjero sin conexión con los Estados Unidos. Sin embargo, el único tribunal que parece haber abordado la cuestión concluyó lo contrario. Un juez de distrito en 1985 resolvió que un ciudadano de Alemania

[661] BARRON, p. 67.
[662] Idem, p. 68, referencia n° 150.
[663] En particular, porque el Congreso, en 1961 eliminó una disposición que limitaba su aplicación sólo "dentro del almirantazgo y jurisdicción marítima de los Estados Unidos y en alta mar, así como dentro de los Estados Unidos".

del Este podría ser procesado bajo las Secciones 793 (b), 794 (a) y 794 (c).[664]-[665]

En ese caso, los acusados no estadounidenses que publiquen materiales que perjudican los intereses de Estados Unidos en formas que son legales en su jurisdicción, podrían ser procesados bajo la ley de EE.UU. estando cubiertos por las garantías sustantivas de la Declaración de Derechos o *Bill of Rights*, por lo tanto la Primera Enmienda sí se les aplica.[666]

En una hipotética demanda contra *The Guardian* o Assange por la publicación de los cables diplomáticos, hace más de cien años la Corte Suprema en uno de los precedentes más importantes que extienden la protección constitucional más allá de las fronteras de Estados Unidos, declaró expresamente que "la libertad de expresión y de prensa", han sido de esos derechos tan "indispensables a un gobierno libre" que se aplican en el extranjero[667].

En *Branzburg v. Hayes (1972)*, se dijo que no es probablemente un argumento plausible plantear que no se aplica la Primera Enmienda a la prensa extranjera. En *United States v. 18 Packages of Magazines* (D.C. Cal. 1964), se estableció que:

---

[664] *United States vs. Zehe (1985).* Por tener (1) la información solicitada y obtenida ilegalmente sobre la defensa nacional de EE.UU., (2) entregó esa información a su propio gobierno, y (3) conspiró para hacerlo con la intención de que la información fuese utilizada en perjuicio de los Estados Unidos o en beneficio de la República Democrática Alemana, todos los cuales fueron delitos cometidos en Alemania del Este o en México.

[665] ELSEA, op. cit., p. 16.

[666] En esta construcción, es posible que los no ciudadanos que participan en la publicación de materiales revelados a ellos por otro estarán sujetos a enjuiciamiento si se puede demostrar que tomaron un papel activo en la obtención de la información. El caso no fue apelado. El acusado, el Dr. Alfred Zehe, se declaró culpable en febrero de 1985 y fue condenado a ocho años de prisión, pero fue negociado como parte de un "intercambio de espías" con Alemania del Este en junio de ese año. ELSEA, op. cit., p. 17.
En: "*WikiLeaks & the First Amendment"*, Bulletin of the American Academy of Arts & Sciences, Spring 2012, p.27, referencia 213 citando a *Yick Wo vs.Hopkins*, 118 U. S. 356, 374 (1886); ver también *Boumediene vs. Bush*, 553 U.S. 723 (2008).

[667] *Downes vs. Bidwell*, 182 U.S. 244, 282-83 (1901). BENKLER, op. cit., p. 36, referencia 218.

"La Primera Enmienda protege a la población de este país... La Primera Enmienda con seguridad fue diseñada para proteger los derechos de los lectores y distribuidores de publicaciones no menos que los de los escritores o impresores. De hecho, la esencia del derecho a la libertad de prensa de la Primera Enmienda no es tanto el derecho de imprimir, sino que el derecho a leer. Los derechos de los lectores no deben ser restringidos debido a la procedencia geográfica de los materiales impresos".[668]

III.4.2.2. ¿El gobierno de EE.UU. podría demostrar el requisito de la intención específica?

Desde este apartado utilizaremos las opiniones de los más destacados profesores de derecho y de abogados expertos en la materia, en específico de Jerome A. Barron, profesor de la Universidad George Washington; Yohai Benkler, profesor de la Universidad de Harvard; Shaina Jones y Jay Ward Brown abogados especialistas en Medios; Jennifer K. Elsea abogada del Servicio de Investigación del Congreso de Estados Unidos; Gabriel Schoenfeld miembro del Instituto Hudson en Washington y del Instituto Witherspoon en Princeton; Stephen Carter profesor de la Universidad de Yale y Geoffrey Stone, profesor de la Universidad de Chicago.

III.4.2.2.a. Posición del Profesor Barron. Primero que todo se refiere a la constitucionalidad de la ley, plantea que es un estatuto que tiene casi cien años y que según los actuales estándares de la Primera Enmienda, el lenguaje de muchas de sus disposiciones es vago y demasiado amplio[669].

Luego, propiamente refiriéndose al punto en cuestión, piensa que el caso *AIPAC* es ilustrativo[670], el juez Ellis se negó a desestimar la acusación según la Ley de espionaje[671], sin embargo al mismo tiempo declaró que un enjuiciamiento exitoso tenía que cumplir con el requisito de probar la intención

[668] ELSEA, op. cit. p. 22, referencia 138.
[669] Barron, op. cit., p. 68, referencia 150.
[670] Idem, referencia 152.
[671] Idem, referencia 155.

específica. “La información debe estar relacionada con la defensa nacional, ser ya sea tangible o intangible, debiendo ser necesariamente aquella cuya divulgación sea potencialmente perjudicial para los Estados Unidos, y el acusado debe saberlo”[672].

Por otra parte, el profesor Barron recuerda que antes que se publicaran los cables diplomáticos Assange se dirigió al Departamento de Estado preguntando acerca de los criterios que podrían enmarcar un actuar correcto o incorrecto de su parte desde el punto de vista estadounidense[673]. El Departamento de Estado se negó a cooperar[674]. Por lo tanto, dice, puede ser difícil demostrar que existió una deliberada intención de dañar a Estados Unidos. Uno podría esperar que su abogado defensor argumente que sus acciones demuestran lo contrario.

Según su postura, incluso si se cumple con el requisito específico de la intención de la Ley de Espionaje, la persecución contra Assange por publicar a través de *WikiLeaks* aún tendría que sobrevivir a la cuestión de la Primera Enmienda.[675]

III.4.2.2.b. Opinión del profesor Shoenfeld. Estima que la ley de Espionaje es problemática, que nunca se ha utilizado para procesar a la prensa, y que al hacerlo se plantearían cuestiones constitucionales graves.[676]

III.4.2.2.c. Posición del profesor Stephen Carter. Según su pensamiento, lo que Assange ha hecho no es muy distinto a que una persona que haya obtenido ilegalmente las declaraciones de impuestos de los principales periodistas, los publique en línea, muestre cuánto dinero gana cada uno, todo

[672] Idem, p. 69, referencia 156.
[673] Idem, p. 69, referencia 157.
[674] Idem, referencia 158.
[675] Idem, p. 69.
[676] En: “*WikiLeaks & the First Amendment”*. [WikiLeaks y la Primera Enmienda]. Bulletin of the American Academy of Arts & Sciences, Spring 2012, p.27.

con el objetivo, se podría decir, de demostrar sus prejuicios. Tal individuo, según Carter es digno de condena, no de celebración. Pero ese actuar cruelmente, o auto-interesadamente, o de modo narcisista, dice el profesor, no debe ser de índole penal, sobre todo cuando de lo que se trata es, sin lugar a dudas, del habla.[677]

III.4.2.2.d. Reflexión de Jones y Ward. Según ellos, parece claro que Assange divulgó documentos relacionados con la defensa nacional a personas que no tenían derecho a recibirlas, que al menos algunos de estos documentos eran secretos, que objetivamente su divulgación tendría el potencial de dañar la seguridad de los Estados Unidos, y que Assange era consciente del carácter secreto de los documentos. Si esto es correcto, y si el juez al que se le asignare el caso adhiere a la articulación de la carga del gobierno razonada por el juez Ellis, entonces la única pregunta que queda es si el gobierno puede demostrar que Assange sabía que la divulgación de los documentos era ilegal, y no obstante ello, procedió, es decir, que actuó con mala intención para desobedecer la ley.[678]

Piensan que, si hubiese sido uno de los medios de comunicación dominantes en Estados Unidos el que dio a conocer los mismos documentos que *WikiLeaks,* respondería esta acusación declarando que su intención era la de informar al público sobre asuntos pertinentes al *self-government*, y que no se violó ni la ley ni se dañó al gobierno. Así se ha interpretado la intención por los tribunales en circunstancias análogas.[679]

Ahora, refiriéndose específicamente a la liberación de los cables diplomáticos y la prueba de la intención específica, citan a Baruch Weiss,

[677] JONES, op. cit., p.139, referencia 115 citando a su vez a Stephen L. Carter, *The Espionage Case Against Assange*, The Daily Beast [en línea] <http://www.thedailybeast.com/articles/2010/12/01/julian-assange-should-espionage-act-be-used-against-him.html> [Consulta: 06/08/2013]
[678] Idem, p. 135.
[679] Idem.

abogado de la defensa en el caso *AIPAC*, que señaló que "mucho antes de la publicación de los cables, [Assange] escribió una carta al gobierno de EE.UU., la que fue entregada a nuestro embajador en Londres, pidiendo sugerencias para sus redacciones. El Departamento de Estado se negó. Assange después escribió otra carta, reiterando que "*WikiLeaks* no tiene absolutamente ningún deseo de poner a las personas individuales en riesgo significativo de daño, ni queremos dañar la seguridad nacional de los Estados Unidos."[680]

III.4.2.2.e. Opinión de Jeniffer K. Elsea abogada del Servicio de Investigación del Congreso. Piensa que existe una amplia autoridad legal para procesar a las personas que provocan la difusión o difunden los documentos en cuestión, siempre y cuando el elemento de intención pueda ser probado y el daño potencial a la seguridad nacional pueda ser demostrado. Dice que, sin embargo, hay una posición interpretativa de la sección 793, que prohíbe la comunicación, transmisión o entrega de información protegida a cualquier persona que no tenga derecho a tomar posesión de ella, que excluye la publicación del material. [681]

Por otra parte, nos dice que el estatuto descrito en el apartado anterior se ha utilizado casi exclusivamente para procesar a personas con acceso a la información clasificada (y la correspondiente obligación de protegerla) que la pusieron a disposición de agentes extranjeros o agentes extranjeros que obtuvieron la información clasificada ilegalmente mientras se encontraban en EE.UU. Argumenta que el Servicio de Investigación del Congreso[682] no tiene conocimiento de algún caso en que un editor de la información obtenida a través de la divulgación no autorizada por un empleado del gobierno haya sido procesado por publicarlo. Es posible que las implicaciones relacionadas con la Primera Enmienda hagan difícil tal acusación, y eso sin hacer mención de las

[680] Idem, p. 136.
[681] ELSEA, op. cit., p. 15.
[682] Congressional Research Service.

contingencias políticas que sobrevendrían basadas en preocupaciones sobre la posible intención de censura por parte del gobierno.[683]

El gobierno tendría la carga de probar la "mala intención" de *WikiLeaks* o Assange, lo que además de ser de suyo complejo, ha sido percibido como un obstáculo para el enjuiciamiento de los periodistas en el pasado.[684]

III.4.3. ¿Las publicaciones de Assange y WikiLeaks están protegidas por la Primera Enmienda?

Más allá de la exigencia de que el gobierno demuestre la intención necesaria para asegurar una condena en virtud de la Ley de Espionaje, lo que como hemos visto, se observa de muy compleja consecución, quedaría, sin embargo, la cuestión de si su aplicación a *WikiLeaks* sería constitucional. Como se ha señalado, los tribunales nunca se han enfrentado directamente con el procesamiento de un órgano de prensa o similar a un periodista individual bajo la ley, al menos no en la era de la moderna jurisprudencia de la Primera Enmienda.[685]

De inmediato emerge la duda de si *WikiLeaks* podría utilizar la garantía que tienen los medios de prensa, entre otras preguntas tales como: ¿Quienes deben hacerse cargo de que los secretos del gobierno sigan siéndolo para integridad de la seguridad nacional? Y ¿Cuál ha sido el daño que las publicaciones de WikiLeaks han provocado en la política exterior de Estados Unidos y a su seguridad nacional? Para ellos volveremos a recurrir a opiniones de la doctrina especializada.

---

[683] ELSEA, op. cit., p.16.
[684] Idem.
[685] JONES, op. cit., p.140.

III.4.3.1. ¿WikiLeaks es parte de la prensa?

III.4.3.1.a. Posición del Profesor Barron. Describe que hoy algunos *bloggers* reciben pases de prensa y participan en las conferencias de prensa presidenciales[686]. Dice que el sitio *web WikiLeaks* existe con el fin de distribuir información, pero que sin embargo algunos sostienen que Assange no es un periodista[687]. Sin embargo, argumenta que la invocación de protección de la Primera Enmienda no requiere que los gobiernos o la sociedad en general aprueben la información que se opta por difundir. Que, establecer el argumento que pretende excluir a *WikiLeaks* de la protección conferida por la garantía de la libertad de prensa debido a que su contenido se transmite a través de la Internet en lugar de a través de las páginas impresas de los diarios, es refutarlo. Este argumento, dice, es especialmente débil en un caso como el de *WikiLeaks*, en el que los medios de comunicación tradicionales han trabajado muy cerca de *WikiLeaks*[688]. La cooperación de estos medios tradicionales sólo ha servido para aumentar el alcance de sus publicaciones.

Plantea que las publicaciones demuestran una interacción entre *WikiLeaks* y la prensa establecida. Cuando los primeros envíos de material sobre la guerra de Afganistán fueron publicados por *WikiLeaks*, la reacción de la prensa tradicional fue de crítica[689]. Los nombres de soldados y otros miembros habían sido revelados y la prensa informó de personas cuya vida se habría puesto en peligro[690].

Luego, dice, al momento de publicarse los archivos relativos a Irak y versiones posteriores de los cables diplomáticos, *WikiLeaks* editó el material, la

[686] BARRON, p. 70, referencia 163.
[687] Idem, referencia 164.
[688] Idem, referencia 165.
[689] Idem, referencia 166.
[690] Idem, referencia 167.

prensa tradicional lo elogió[691], tuvo acceso previo al material que se publicaría[692], por lo que en lugar de competir, *WikiLeaks* aparentemente había decidido cooperar con la prensa establecida, y que de hecho, *WikiLeaks* se había convertido en una especie de prensa adjunta.

Argumenta que, en casos como este, para él se debe aplicar un "examen riguroso", pues un interés gubernamental apremiante podría llegar a prevalecer sobre las consideraciones de la Primera Enmienda[693].

Si Assange es procesado, estima que lo más probable es que alegue en que el sitio *web WikiLeaks* es parte de la prensa. Cita a Baruch Weiss que señaló que ni el *Washington Post* ni el *New York Times* están siendo investigados por publicar el mismo material que Julian Assange publicó en *WikiLeaks*[694]. La razón de esto sería clara: la Primera Enmienda les da la garantía de la libertad de prensa. Weiss dice que la práctica del Departamento de Justicia ha sido la de "abstenerse de introducir acusaciones sobre las fugas contra los medios de comunicación tradicionales"[695]. Sin embargo, Julian Assange está siendo investigado. Weiss sugiere que "(el procurador general) Holder puede sentirse animado a dirigirse contra *WikiLeaks*, (sólo) porque no tiene el aspecto o la impresión de tratarse de un medio de comunicación tradicional"[696].

III.4.3.1.b. Reflexión del Profesor Benkler. Para él la diferencia más obvia entre *WikiLeaks* y los medios de comunicación tradicionales es la identidad de la organización. Estos últimos nos son culturalmente familiares como principales medios de comunicación, tenemos una suposición cultural general de su cultura

[691] Idem, p. 71, referencia 168.
[692] Idem, referencia 169.
[693] Idem, referencia 170.
[694] BARRON, op. cit., p. 68, referencia 160.
[695] Idem, referencia n° 161.
[696] Idem, referencia n° 162.

organizacional: se preocupan por obtener los datos correctos, y de ser "responsables", dice, en la presentación de las noticias. Expresa que entonces, la línea divisoria importante es entre los medios y los periodistas establecidos, por un lado, y la cultura descentralizada, informal y cuasi-formal de expresión en Internet. ¿Qué podría explicar esta diferencia? se pregunta. La intuición, dice, probablemente tomaría una forma análoga a la expresión formulada por Jonathan Klein, quien, poco antes de asumir como presidente de CNN EE.UU. dijo que "no podría haber un contraste más marcado entre las múltiples capas de pesos y contrapesos (de un medio de prensa) y un chico sentado en su sala de estar en pijama escribiendo lo que piensa", haciendo referencia a los bloggers que habían exhibido un informe de 60 minutos de la historia militar del presidente George Bush. Klein ya no conduce CNN EE.UU., pero el tratamiento desdeñoso hacia la blogósfera desde los medios tradicionales no ha desaparecido.[697]

Benkler recuerda que la cobertura a *WikiLeaks* del propio *New York Times* se combina con retratos poco halagadores de Julian Assange[698]. Piensa que estas descripciones parecen representar una profunda ansiedad y crisis de identidad de los medios tradicionales, tal vez exhibiendo un miedo existencial a que los días de gloria de su profesión hayan pasado, tal vez sencillamente por envidia por el hecho de que la mayor primicia de 2010 fue generada por alguien que no era miembro del club. Cualquiera que sea la razón de este retrato poco favorecedor, dice, no puede constituir la base de un principio constitucional.[699]

Plantea, citando a la Corte Suprema que:

[697] BENKLER, p.37.
[698] A quien el periódico describió variadamente como "hombre perseguido", que "registra en hoteles bajo nombres falsos, se tiñe el pelo, duerme en los sofás y pisos, y usa efectivo en lugar de tarjetas de crédito, a menudo prestado de amigos", o que usaba una "camisa blanca sucia, zapatillas deportivas y calcetines blancos sucios que se derrumban alrededor de sus tobillos. Olía como si no se hubiera bañado en días".
[699] Idem, p.38.

"La libertad de prensa es un derecho tanto del panfletario solitario que utiliza papel carbón o un mimeógrafo, como de la gran editorial metropolitana que utiliza los últimos métodos de fotocomposición"[700].

La organización de "frenos y contrapesos" institucional-procesales de los que Klein habló, dice, no pueden sostener una distinción que haga la diferencia constitucional.[701]

La diferencia entre medios de Internet y los medios de comunicación tradicionales no puede, entonces, ser el tamaño o la complejidad organizativa. Funcionalmente, reflexiona, es más importante proporcionar protección constitucional sólida a los miembros más débiles de la Internet, que tienen menos visibilidad pública y recursos para resistir la presión de los funcionarios del gobierno, de lo que es hacer hincapié en los derechos de los miembros de un ente organizativa y económicamente más fuerte.[702] Aunque el director ejecutivo del *New York Times* haga hincapié en que ve a Assange como "una fuente", enfáticamente no un socio, y no realmente un periodista, esta negación sentenciosa de la membresía en el club no hace una diferencia constitucional.[703]

Cita el caso *Von Bulow vs. Von Bulow (2nd Cir. 1987)*, en que la Corte de Apelaciones sostuvo que:

"el individuo que reclama el privilegio debe demostrar... la intención de utilizar el material - buscado, reunido o recibido - para difundir información al

[700] Idem, referencia 227 *Branzburg v. Hayes*, 408 U.S. 665, 704 (1972).
[701] Idem, p. 38.
[702] Idem. "Cuando el senador Bunning y el representante Kyl llaman a la revelación del *New York Times* del programa de espionaje interno *NSA* "traición a la patria", había poco riesgo de éxito de un proceso penal contra el *NYTimes*, o que su editor se llegara a encontrar bajo arresto domiciliario, que llevase un brazalete en el tobillo . El enorme poder económico, social y cultural del *New York Times* implica que las garantías constitucionales no tendrían que "patear" para evitar tal eventualidad. Lo mismo no es necesariamente cierto para un hombre a quien el Vice Presidente de EE.UU. describe como un "terrorista de alta tecnología", y que el *New York Times* describe como "un hombre perseguido", mientras que su director ejecutivo hace hincapié en que lo ve como "una fuente", enfáticamente no un socio, y no realmente un periodista."
[703] Idem, p.39.

público y que esa intención existía al inicio del proceso de recopilación de noticias."[704]

El tribunal concluyó subrayando, dice, que la membresía en el club de periodistas establecidos no es necesaria para la protección[705].

El elemento definitorio fundamental entonces, para Benkler, sería la intención en el momento de la recolección y su función, no el modo de difusión: la intención de recolectar información para su difusión pública. Para el Profesor, simplemente no puede haber la duda más remota que todo el propósito de *WikiLeaks* es la recopilación de información para la difusión pública y el uso de los medios de comunicación tradicionales como la vía principal destaca este hecho, aunque no es constitutivo o un elemento necesario de la defensa. El profesionalismo, amabilidad, o la higiene personal del periodista no son pertinentes para la investigación. El interés de que se trata no es individual, argumenta, sino que sistémico: es "El interés de la sociedad en la protección de la integridad del proceso de recopilación de noticias, para garantizar la libre circulación de la información al público."[706] Tampoco para él es relevante si su interés es o no perjudicar al gobierno de Estados Unidos[707].

---

[704] Idem.

[705] "Aunque la experiencia previa como periodista profesional puede ser una evidencia persuasiva de la intención presente de reunir para los efectos de difusión, no es condición *sine qua non*. La carga, de hecho puede ser sostenida por alguien que es un novato en el campo. Además, la protección contra la divulgación puede ser solicitada por alguien a quien no se asocia tradicionalmente con la prensa institucionalizada porque "[l]a función informativa afirmada por los representantes de la prensa organizada (...) También se lleva a cabo por los profesores, encuestadores políticos, novelistas, investigadores, académicos y dramaturgos". Idem, p. 38-39, referencia 238, citando 274 U.S. 357 (1927).

[706] Idem, referencia 241.

[707] El propósito de la protección de la prensa es sistémico y funcional - para servir a un público más ilustrado, que es condición previa para que una democracia funcione bien. La motivación que impulsó a cualquier individuo dado para avanzar en ese objetivo es totalmente irrelevante para la cuestión central. Un periodista no se mide por el hecho de que investiga y publica con el fin de servir a la democracia, engrandecer su nombre, o hacer dinero, *Fox News* no sería menos merecedor de la Libertad de prensa si se encontraran una serie de memorandos internos que revelen que su primer motivo era el de socavar la capacidad del presidente Obama para gobernar, en lugar de informar al público. Indagar en las motivaciones políticas o personales de los oradores abre la puerta a la forma más perniciosa de la censura-la definición de algunas motivaciones políticas como bases legítimas para el habla, y otras como ilegítimas no son elegibles para la protección. Un reportero que opera por convicción política es tan protegido como

Llega, entonces, a la conclusión de que, como cuestión de doctrina de la Primera Enmienda, *WikiLeaks* tiene derecho a la protección disponible para una amplia gama de miembros del cuarto poder. Como cuestión valorativa en la Primera Enmienda, dice, esta niega privilegiar al *New York Times* sobre *WikiLeaks* por el derecho de la continuidad del acceso del público a un flujo constante de información veraz y relevante sobre el funcionamiento interno de su gobierno.[708]

Sostiene que, la esfera pública en red se desarrolla como un conjunto diverso de actores, desde *bloggers* individuales, pasando por organizaciones no lucrativas como la Fundación *Sunlight*, pequeñas publicaciones en línea comerciales y grandes grupos descentralizados de activistas políticos como *DailyKos* o *Townhall*, que vienen a jugar un papel cada vez más importante en la construcción de la esfera pública, siendo de importancia funcional el divorciarse de la protección constitucional que se entendía desde la medida en que el solicitante formaba parte del modelo del siglo XX de los grandes medios de comunicación.[709]

Agrega, en términos formales que en marzo de 2010 *Wikileaks* publicó un informe de 2008 del Pentágono que decía que *Wikileaks* era una amenaza, al tiempo que lo reconoce como una fuente de periodismo de investigación crítica de las adquisiciones militares de EE.UU. y de su conducta en la guerra[710]. El reconocimiento del rol periodístico que *Wikileaks* juega queda claro para la discusión en varios ejemplos de publicaciones de *Wikileaks* en que el

---

un reportero que busca hacer dinero, convertirse en una celebridad, o humildemente servir al interés público. Idem, p. 41.

[708] Idem.

[709] Idem, p. 42.

[710] Idem, p. 5, referencia 19.

informe describe repetidamente como “los artículos de noticias” y describe a Julian Assange como “escritor del *staff* extranjero.”[711]

Para él, no es sostenible dar a *Wikileaks* y Assange un tratamiento diferente que al *New York Times* y sus periodistas con fines de censurar previamente o de modo ex post procesar penalmente. Ello, en consonancia con su interpretación de la Primera enmienda y la protección de la libertad de prensa. Según él, un enjuiciamiento a *WikiLeaks* o Assange seguramente no prosperará bajo la actual doctrina de la Primera enmienda. Añade que, en el improbable caso de que la persecución tenga éxito, sólo lo haría a costa de empeorar la Primera Enmienda desde la perspectiva de la libertad de prensa en la era de la Internet.[712]

III.4.3.1.c. Posición de Jones y Ward. Plantean con respecto a la versión de abril de 2010 del video “asesinato colateral”, sería difícil argumentar que *WikiLeaks* no realiza ninguna función periodística tradicional: No sólo edita y titula el video, sino que, al parecer, envió personal a Irak para entrevistar a los testigos iraquíes sobre el incidente para asegurar la veracidad de la información, para luego lanzarlo. Algo que *Reuters* había intentado, sin éxito, durante años, fue un hecho ampliamente cubierto por organizaciones de noticias en Estados Unidos y en el extranjero.[713]

No obstante estos hechos, plantean que algunos comentaristas se han resistido a clasificar a *WikiLeaks* como una organización de noticias. Por lo general, estos comentaristas se enfocan en un eventual desplazamiento de material sin mediación de fuentes, la falta de transparencia en el proceso de

[711] Idem, p. 6, referencia 29.
[712] Idem, p. 3 - 4.
[713] JONES, op. cit, p. 137.

investigación, en la falta de responsabilidad atribuible a su edición de secretos y en la existencia misma de la organización.[714]

Cuando *WikiLeaks* publicó los documentos de Afganistán en julio de 2010, se retuvieron unos 15.000 que se declararon especialmente sensibles, pero no se eliminaron los nombres de fuentes de inteligencia afganos de algunos de los documentos publicados. "La ex mano derecha" de Assange y *WikiLeaks*, el ex portavoz Daniel Domscheit-Berg ha afirmado públicamente que Assange actuó con negligencia al respecto.[715]

Es significativo, dicen, que teniendo en cuenta el principal obstáculo para la invocación de la ley de Espionaje contra la prensa, un periodista que trabajó con Assange ha alegado expresamente que este deseaba dañar a los aliados de EE.UU., en específico, David Leigh de *The Guardian,* dice que habló con Assange advirtiéndole de que personas podrían verse peligrosamente expuestas por estas filtraciones sin edición. Supuestamente el periodista dijo que tenían que hacer algo, a lo que Assange habría respondido: "Estas personas eran colaboradores, informantes. Ellos merecen morir."[716]

Plantean que es difícil discernir un argumento convincente de que cualquiera de las diferencias fácticas entre *WikiLeaks* y las "organizaciones típicas de noticias" importe cuando se trata de buscar refugio bajo la Primera Enmienda. Correctamente entendida, argumentan, la Primera Enmienda "no se preocupa si *WikiLeaks* es un acreditado distribuidor de noticias, un grupo de *hackers* "de sombrero negro" o un circo ambulante", precisamente porque la protección que ésta ofrece "depende de lo que *WikiLeaks* publica, no de lo que es".[717] De hecho, es bien aceptado, dicen, que "la prensa en su connotación

[714] Idem.
[715] Idem.
[716] Idem, p.139.
[717] Idem, referencia 116 citando a su vez a Andy Greenberg, *Is WikiLeaks a Media Organization? The First Amendment Doesn´t Care*, FORBES [en línea]

histórica comprende todo tipo de publicación que ofrece un vehículo de información y de opinión."[718]

Exponen que si existe una diferencia significativa que se pueda elaborar entre *WikiLeaks* y la prensa tradicional a efectos de la aplicación de la Ley de Espionaje, podría ser sólo la intención específica del editor con respecto a la ley penal en cuestión.[719]

Además, agrega el principio *"Daily Mail/Florida Star/Bartnicki" en el* análisis, pues más allá de la exigencia de que el gobierno demuestre la intención para lograr una condena en virtud de la ley de Espionaje, queda, sin embargo, la cuestión de si la aplicación de las prohibiciones a *WikiLeaks* sería constitucional en las circunstancias específicas de las fugas. Como se ha señalado, los tribunales nunca se han enfrentado directamente con el procesamiento de un órgano de prensa o similar a un periodista individual bajo la ley de espionaje, al menos no en la era de la moderna jurisprudencia de la Primera Enmienda.[720]

En una serie de casos que comienzan con *Smith vs. Daily Mail* en 1979, la Corte Suprema en varias ocasiones ha subrayado que:

"la información veraz sobre un asunto de interés público" recibe muy amplia protección ante la responsabilidad penal o civil.[721]

Conocido como "el principio *Daily Mail*", esta exigencia constitucional de base fue explicada recientemente por la Corte Suprema en *Bartnicki vs.*

<http://www.forbes.com/sites/andygreenberg/2011/04/21/is-wikileaks-a-media-organization-the-first-amendment-doesnt-care/> [Consulta: 06/08/2013]

[718] Idem, referencia 117 citando a su vez *Lovell vs. City of Griffin*, 303 U.S. 444, 452 (1938).

[719] Idem, p.140.

[720] Idem.

[721] Idem, referencia 120 acerca de *Smith v. Daily Mail*, 443 U.S. 97, 103 (1979) en el contexto de la afirmación de que un periódico publicó el nombre del agresor de menores, sostiene que "si un periódico obtiene legalmente información veraz acerca de un asunto de importancia pública, luego los funcionarios estatales no podrán sancionar constitucionalmente la publicación de la información, en ausencia de la necesidad de promover un interés estatal de primer orden".

Vopper[722] un caso que surje bajo la ley federal de Escuchas Telefónicas[723] que tipifica como delito y crea una acción civil para la interceptación ilegal y la difusión de comunicaciones por cable o inalámbricas[724]. Describen que cuando la discusión se fundamenta sobre información veraz acerca de un asunto de importancia pública, la Corte reafirmó:

> "entonces los funcionarios del Estado no pueden castigar constitucionalmente la publicación de la información, en ausencia de una necesidad… de primer orden"[725].

De importancia para Assange, el Tribunal Supremo también hizo hincapié en que el grado de protección que ofrece la Primera Enmienda en este sentido no varía en base a la identidad del hablante o la percepción de la utilidad social de la información difundida.[726] Además, dicen, refiriéndose a la circunstancia en la que el editor obtiene la información sabiendo que la fuente ha actuado ilegalmente en la obtención o diseminación, el Tribunal directamente sostuvo que "la conducta ilegal de un extranjero no es suficiente para eliminar la protección de la Primera Enmienda al debate sobre un asunto de interés público"[727]. Cabe destacar que esta protección dejaría de operar, dijo la Corte, cuando el editor va más allá de saber que acepta material obtenido ilegalmente por otro, llegando a la participación real en la obtención ilegal de material, lo que constituiría *hacking* en su matiz descrito como delito penal.[728] Esto explica según ellos la posición en la propia *web* de *WikiLeaks* y en los sitios de las organizaciones que han lanzado modelos similares, de negar expresamente la

[722] *532 U.S. 514 (2001).*
[723] *Wiretapping Act.*
[724] JONES, op. cit., p.140.
[725] Idem, p. 141, referencia 122 *Bartnicki vs. Vopper*.
[726] Idem, referencia 123.
[727] Idem, referencia 124.
[728] Idem, referencia 125.

intención de inducir (y en algunos casos, desconocer la voluntad de aceptar los resultados de) revelaciones de fuentes ilegales.[729]

Reflexionan que, tal vez la analogía más cercana a *WikiLeaks* en estos aspectos es presentada por *Jean v. Mass. State Police en que se aplicó el precedente Bartnicki*[730].

Suponiendo que, en el caso de Assange, hubiese actuado conjuntamente con las fuentes de *WikiLeaks* en sus actos iniciales presuntamente ilegales de adquisición y divulgación, viciando la aplicación del principio *Daily Mail* en primera instancia, y suponiendo que el gobierno podría cumplir en lo demás con la carga de la prueba ¿El gobierno tendría éxito en demostrar que la aplicación de la Ley de Espionaje a Assange sirve legítimamente a un interés de "primer orden"? La protección de la seguridad nacional, incluidos los secretos necesarios para la seguridad, parecen claramente calificar como un interés nacional de primer orden[731]. La pregunta más precisa sería si el contenido de los documentos publicados por *WikiLeaks* reflejan esos intereses. Por ejemplo, un comentarista ha argumentado que, si los cables revelan los nombres de agentes secretos en Afganistán o Irak, o se refieren a planes de guerra futuros o contienen algo referido a prácticas similares, el estándar de la norma podría superarse.[732]

III.4.3.1.d. Opinión del abogado Elsea del Servicio de Investigación del Congreso. Opina que el hecho de que *WikiLeaks* no sea una organización de recopilación de noticias y de publicaciones tradicional probablemente hará poca

[729] Idem, p. 141.
[730] Idem, referencia 126. 492 F.3d 24 (1st Cir. 2007). Allí, Mary Jean publicó en Internet una grabación de audio y video de un arresto y allanamiento residencial sin orden judicial, a pesar de su conocimiento de que la grabación se había hecho ilegalmente. Ver en este trabajo, a propósito de las decisiones relevantes de la jurisprudencia estadounidense.
[731] Idem, referencia 132 citando a su vez el caso *Rosen.*
[732] Idem, referencia 133 citando a su vez a Andy Sellars, *WikiLeaks and the First Amendment*, ANDY ON THE ROAD [en línea] <http://andyontheroad.wordpress.com/2010/12/11/wikileaks-and-the-first-amendment/> [visitado el 12-08-2013]

diferencia en el análisis de la Primera Enmienda. Reflexiona que el Tribunal Supremo no ha establecido límites claros entre la protección de la expresión y de la prensa, ni ha tratado de desarrollar criterios para determinar lo que constituye "la prensa", para poder calificar a sus miembros con privilegios que no están disponibles para cualquier persona.[733]

III.4.3.2. ¿Quién es el garante de que los secretos del gobierno sigan siéndolo?

Mucho optimismo se generó a propósito de que la libertad de prensa se expandiría de nuevo en 2008, cuando el candidato presidencial Barack Obama prometió aumentar la transparencia y reducir los secretos gubernamentales. Sin embargo el presidente Obama ha seguido una tendencia hacia un mayor secreto del gobierno, incluso en comparación con gobiernos anteriores. De acuerdo con la Oficina de Supervisión de Seguridad de la Información, la agencia federal que supervisa los sistemas de clasificación del gobierno, el costo anual de la clasificación se ha elevado a más de 10,7 mil millones de dólares sobrepasando el umbral de $ 10 mil millones por primera vez, porque muchas de las decisiones gubernamentales que solían será públicas están siendo clasificadas como secretos.[734]

En 2010, aproximadamente 224.000 documentos fueron clasificados, significando un aumento del 22% respecto a 2009.[735]

Las solicitudes motivadas por la ley de Libertad de Información también han aumentado en respuesta al creciente secretismo gubernamental. Hubo más

[733] ELSEA, op. cit., p. 22, referencia 138 que recomienda ver también Congressional Research Service, The Constitution of the United States: Analysis and Interpretation, Sen. Doc. n° 108-17, at 1083-86 (2002), [en línea] <http://crs.gov/conan/default.aspx?mode=topic&doc=Amendment01.xml&t=2|3.> [revisado sin resultados positivos el 13-08-2013]
[734] MILLER, Judith. En: "*WikiLeaks & the First Amendment*". Bulletin of the American Academy of Arts & Sciences, Spring 2012, p. 20.
[735] Idem.

de medio millón de solicitudes en 2010, o 40.000 más que en 2009, y la burocracia del gobierno respondió a 12.400 solicitudes menos que en el año anterior. Así que, más solicitudes se están haciendo, y menos están siendo procesadas.[736]

Pero hay algo peor: que este gobierno ha invocado el secreto de Estado más que cualquier otro en los tiempos modernos, incluyendo la administración del presidente Bush, en lugar de responder a las solicitudes de información clasificada. El presidente Obama ha solicitado el privilegio con respecto a la vigilancia de la Agencia de Seguridad Nacional, las escuchas telefónicas ilegales, y otras actividades.[737]

III.4.3.2.a. Reflexión del Profesor Benkler. Para él *WikiLeaks* en ningún caso tiene que cumplir con el rol de conservar o cuidar que los secretos de la Administración no sean conocidos. Dice, a propósito también de los *Pentagon Papers*[738] que: "Este poderoso ejecutivo tiene la responsabilidad de mantener sus propias operaciones con suficiente seguridad y sabiduría para asegurarse de que sólo lo que necesita clasificar es de hecho clasificado, y lo que se clasifica no consigue ser filtrado."[739]

III.4.3.2.b. Posición del Profesor Posner. Estima que, por un lado, *WikiLeaks* hizo un esfuerzo por proteger la identidad de las personas que podrían estar en peligro por las fugas. Piensa que ese es uno de los intereses más importantes, y que, por otro lado, también hay algunos secretos militares

[736] Idem.
[737] Idem.
[738] BENKLER, op. cit., p. 36. También a propósito de los Papeles del Pentágono hace la distinción de que en ese caso el punto de preocupación era la censura previa, en cambio, nuestro objeto de estudio son las posibilidades del eventual juicio y éxito de un procedimiento contra Assange y se hace una pregunta ¿Creemos que un tribunal que consideró que la Primera Enmienda requiere que a los periódicos se les permitirá publicar simplemente permitiría al gobierno procesar y encarcelar a los periodistas después de los hechos? Eso sería una burla a la protección e impondría mucho mayor enfriamiento en la publicación que el riesgo de una medida cautelar." Idem.
[739] Idem, p. 34.

sobre planes, diseño, armas y capacidades que el gobierno debe mantener en secreto, si puede. Además estima que esta categoría constituye una fracción muy pequeña de toda la información clasificada[740]-[741]. Finalmente se posiciona contra la clasificación excesiva de información y documentos porque hace que los esfuerzos por protegerlos sean ridículos.[742]

III.4.3.2.c. Opinión del profesor Schoenfeld[743]. Dice que para mantener la seguridad del país, el gobierno genera una gran cantidad de secretos de muchos tipos. Dice también que no se pueden dar a conocer los métodos de inteligencia para rastrear ni revelar las vulnerabilidades de nuestros puentes, túneles y edificios. Existe, plantea, una obligación absoluta de mantener la información en secreto, como los planos de armas nucleares o de las fórmulas para la producción de ántrax en aerosol.

Pero, sostiene que de la misma manera está igualmente en juego el carácter de la democracia estadounidense. Dice, que vivimos en una sociedad abierta en la que el secreto es la antítesis del ideal democrático. El secreto podría ser utilizado para cubrir la corrupción y el delito. Eso así como, dice, dependemos de la libertad de prensa para que se nos proporcione información acerca de lo que el gobierno está haciendo a nuestro nombre, incluyendo algunas de las cosas que están en secreto. De hecho, asegura, gran parte de lo que leemos en los periódicos acerca de los asuntos exteriores se basa en la presentación de informes sobre secretos de Estado. Manifiesta que la

[740] POSNER, En:"*WikiLeaks & the First Amendment"*, op. cit., p.22.
[741] Idem. El profesor Posner además nos cuenta cierta anécdota: "Una vez fui conducido a una agencia para dar una charla del Día de la Ley, y el funcionario que me escoltaba mencionó que el director de la agencia estaría encantado de responder a cualquier pregunta que pueda tener. Cuando le dije que yo no tenía una autorización de seguridad, dijo que no importaba, porque yo era juez (...) Cuando llegué, me dieron un tour y durante su transcurso me mostró varios documentos clasificados. Lo interesante fue que no había ninguna razón para la que la mayoría de esos documentos hayan sido clasificados (...) Así, no sólo hay información de gobierno que implica la identidad de personas que podrían estar en peligro y que realmente pueda ser útil para un enemigo saberlo, por lo que debería mantenerse en secreto, pero esta representa sólo un pequeño porcentaje de todos los documentos clasificados. Idem, p.23.
[742] Idem, p.23.
[743] SHOENFELD, En:"*WikiLeaks & the First Amendment"*, op. cit., p. 24 y 25.

publicación periódica de los secretos es parte del sistema estadounidense, y que esa es la manera en que debe ser.

Siguiendo con su razonamiento plantea que, así como nosotros queremos una prensa para informar sobre secretos, esta debe hacerlo bajo el imperio de la ley. Es decir, la prensa - que por cierto, dice, incluye *WikiLeaks* - ha de ser susceptible de acciones de la fiscalía cuando viola las leyes que regulan el secreto. Luego, se hace la siguiente pregunta: ¿La existencia de estas leyes significa que los periodistas deben ser procesados cada vez que publican un secreto de Estado? Y responde: por supuesto que no. Dice que es un hecho reconocido el que el gobierno de EE.UU. utiliza el sello secreto promiscuamente. Por lo tanto el dilema no sería si la prensa siempre debe ser procesada por publicar secretos, sino que sería si la prensa puede ser procesada cuando publica secretos que ponen al país en peligro.

Da como ejemplo del daño que se puede causar a un país, el ocurrido durante la Primera Guerra Mundial, en la que el *Chicago Tribune* publicó un artículo sugiriendo que Estados Unidos había descubierto los códigos de la marina japonesa. El gobierno en un principio quiso actuar utilizando la ley de Espionaje, pero luego decidió retirar los cargos para no darle mayor publicidad al artículo. En 2006, *The New York Times* reveló el funcionamiento de un programa de lucha contra el terrorismo que seguía el movimiento de fondos de *al-Qaeda*. El programa era legal y operaba bajo órdenes lícitas. La publicación causó que una de las principales fuentes sobre *al-Qaeda* se secara.

Luego, a propósito de *WikiLeaks*, dice que en nombre de la transparencia, se han arrojado a la Internet indiscriminadamente miles de documentos secretos, en muchos casos, completamente sin editar, aunque muchos de ellos son inocuos.

Algunos, dice, claramente ayudan a entender mejor el papel de EE.UU. en el mundo, pero otros, estima, hacen un grave daño. Da el ejemplo de un documento publicado por *WikiLeaks* que describiría los dispositivos de interferencia empleados por los soldados estadounidenses en Irak para codificar las señales utilizadas por los insurgentes para detonar bombas en las carreteras desde una ubicación remota. El documento habría dado información específica sobre cómo funcionaban y qué frecuencias se bloqueaban. Luego se hace la siguiente pregunta: ¿Hay alguna persona razonable que crea que debería ser legal publicar las contramedidas secretas que nuestros soldados utilizan para evitar volar por los aires en el campo de batalla? ¿La prensa es libre de revelar la identidad de los agentes de la CIA encubiertos? ¿Quién decide esto? Plantea que en una democracia, la gente llega a decidir, y lo que el pueblo estadounidense ha decidido, se manifiesta a través de las leyes aprobadas por sus representantes electos, y la decisión, según su opinión es que la publicación de ciertos tipos de secreto son susceptibles de órdenes de procesamiento. Habrían decidido, según sus palabras, que la Primera Enmienda no es un pacto suicida.[744]

III.4.3.3. ¿Se expuso intencionalmente la seguridad nacional de EE.UU.?

III.4.3.3.a. Opinión del profesor Posner[745]. Cree que las filtraciones han sido en realidad un beneficio. Las filtraciones, para él, demuestran que mientras el número de víctimas fue algo mayor que el que las personas creían, la situación no era tan mala como podría haber sido. Según él, las filtraciones

[744] El profesor Geoffrey STONE no está de acuerdo con el razonamiento, estima que no es del todo claro que se apoye castigar las expresiones meramente porque causen daño. Estima que la evaluación del discurso o relato también tiene importancia.
A lo que SHOENFELD responde que "en cuanto al secreto de seguridad nacional y la cuestión de los daños, vamos a tomar un ejemplo que creo que todos podemos estar de acuerdo: que la publicación de las identidades de los agentes encubiertos de la CIA puede causar daño a las personas. En efecto, el Congreso actuó para que sea ilegal publicar los nombres." Idem.

[745] En: "*WikiLeaks & the First Amendment*", Bulletin of the American Academy of Arts & Sciences, Spring 2012, p. 22.

revelan que las bajas civiles fueron algo peores de lo que se suponían, pero no mucho peores.

También valora positivamente en específico las filtraciones diplomáticas, en el sentido que estas les dirían a los gobiernos extranjeros lo que realmente piensa el gobierno de EE.UU.[746]. Dice que Estados Unidos sigue siendo muy poderoso, y que si estos gobiernos extranjeros saben que EE.UU. está enterado que ellos están minando los intereses norteamericanos, eso sería útil para Estados Unidos[747].

III.4.3.3.b. Posición del profesor Stone. Estima que las razones por las que los funcionarios del gobierno defienden el secreto son muchas y variadas. Van desde las verdaderamente convincentes hasta las notoriamente ilegítimas: A veces, dice, efectivamente es por temor a que la divulgación de cierta información pueda perjudicar gravemente la seguridad de la nación, como la presentación de planes detallados de batalla en su víspera. A veces, simplemente porque no quieren hacer frente a la crítica pública de sus decisiones. Otras, porque la revelación expondrá su propia incompetencia, estupidez o maldad.[748]

Piensa también, que la contribución de la divulgación al discurso público puede variar ampliamente dependiendo de la naturaleza de la información y las circunstancias. La divulgación de cierta información clasificada puede ser extremadamente valiosa para el debate público, por ejemplo, la revelación de programas de gobierno posiblemente ilegales o inconstitucionales, como el uso secreto de interrogatorios coercitivos o la autorización secreta de vigilancia

[746] "el hecho de que el gobierno mexicano sepa lo que pensamos de su ejército, y que Pakistán sepa lo que pensamos acerca de sus relaciones con los talibanes y con China, es toda una ventaja para nosotros." Idem.
[747] Dice que "se podría hacer una analogía con el espionaje mutuo durante la Guerra Fría, en la que nuestro espiar y el recíproco de la Unión Soviética redujo la probabilidad de una guerra real." Idem.
[748] STONE, Geoffrey, *"WikiLeaks, the Proposed SHIELD Act, and the First Amendment"*. [WikiLeaks, la Ley SHIELD propuesta y la Primera Enmienda]. Journal of National Security Law & Policy, [Vol. 5:105 2011], p. 107.

electrónica generalizada. La revelación de otra información confidencial, sin embargo, podría ser de poco o ningún valor para el legítimo debate público, por ejemplo, la publicación de las identidades específicas de los agentes estadounidenses encubiertos en Irán por ninguna otra razón que la exposición.[749]

El verdadero dilema, según Stone, surge cuando la divulgación pública de información secreta es tanto perjudicial para la seguridad nacional, como valiosa para el debate público. Invita a hacer la siguiente suposición: el gobierno inició un estudio sobre la eficacia de las medidas de seguridad en las centrales nucleares del país. El estudio llega a la conclusión de que varias plantas de energía nuclear son especialmente vulnerables a ataques terroristas. Por un lado, la publicación del informe revelaría vulnerabilidades a los terroristas. Por otro, podría alertar al público sobre la situación para que los ciudadanos puedan presionar a los funcionarios del gobierno para remediar los problemas, y mediante la autonomía de los ciudadanos soliciten rendir cuentas a los funcionarios públicos que están garantizando su seguridad. ¿El estudio debería mantenerse en secreto o debería ser divulgado al público? En teoría, plantea, habría simplemente que establecer si el valor de la exposición a la deliberación pública informada supera su peligro para la seguridad nacional. Pero luego, dice que sería simplificar demasiado el análisis, siendo extremadamente difícil medir objetiva, coherente y predeciblemente el “valor” de la divulgación o su “peligro” para la seguridad nacional.[750]

Siguiendo con su argumentación plantea: ¿Quién debería decidirlo? Pensemos primero en personas comunes que no sean empleados públicos. ¿Serán legalmente responsables por revelar información a otro con el propósito

[749] Idem, p. 108.
[750] Idem.

de publicarla? ¿Los derechos de la Primera Enmienda de los empleados públicos son diferentes?[751]

En general, dice, una persona común y corriente tiene un amplio derecho a revelar información a los periodistas u otras personas con fines de publicación. Sin embargo, existen limitaciones.[752]

¿Cuándo podría el gobierno prohibir a un individuo u organización la publicación o difusión de información clasificada filtrada ilegalmente? Dice que en toda la historia de Estados Unidos, el gobierno nunca ha enjuiciado con éxito a nadie (que no sea un empleado del gobierno) para impedir la difusión pública de dicha información.[753]

Describe que debido a que nunca ha existido un procesamiento exitoso, el Tribunal Supremo nunca ha tenido ocasión de pronunciarse sobre este tipo de caso. Lo más cerca que ha llegado a tal situación fue en los *Pentagon Papers*, en el que el Tribunal de Justicia declaró inconstitucional el esfuerzo del gobierno para prohibir la publicación. La opinión del juez Stewart capta la opinión de la Corte: "Se nos pide", escribió, "impedir la publicación. . . de material que el Ejecutivo insiste en que no debería hacerse, en el interés nacional. Estoy convencido de que el Ejecutivo tiene razón con respecto a algunos de los documentos en cuestión. Pero no puedo decir que la divulgación

[751] Idem, p.109.

[752] En primer lugar, el Tribunal Supremo ha reconocido desde hace tiempo que hay ciertas "clases limitadas de expresión", tales como las declaraciones falsas de hechos, obscenidades y amenazas, que "no son parte esencial de cualquier exposición de ideas" y, por tanto, tal expresión puede restringirse sin satisfacer las exigencias habituales de la Primera Enmienda. En segundo lugar, los particulares pueden contraer voluntariamente con otros particulares la obligación de limitar su discurso. La violación de dicho acuerdo privado puede ser punible como un incumplimiento de contrato. En tercer lugar, puede haber situaciones, de todas formas excepcionales, en la que una persona da a conocer previamente la información no pública a un periodista en circunstancias en que la publicación sería tan peligrosa para la sociedad que el individuo puede ser castigado por revelar la información al periodista con fines de mayor difusión. En general, sin embargo, la Primera Enmienda garantiza a los individuos una amplia libertad para compartir información con otras personas con fines de publicación. Idem, p. 109 - 110.

[753] Idem, p.113.

de cualquiera de ellos seguramente resultará en un daño directo, inmediato e irreparable a nuestra nación o a su gente"[754].

Así, en el caso de los Papeles del Pentágono, la Corte sostuvo que aunque los funcionarios electos tienen amplia autoridad para mantener la información en secreto clasificado, una vez que la información llegue a otras manos el gobierno sólo tiene autoridad limitada para evitar su ulterior difusión.[755]

Finalmente subraya que el juez Stewart observó en el caso de los Papeles del Pentágono que, a pesar de que la publicación de algunos de los materiales podrían dañar "el interés nacional", su difusión no podía constitucionalmente prohibirse salvo que su divulgación implicase "sin duda como resultado directo, inmediato e irreparable daño a nuestra nación o de sus personas". Así, plantea que en primer lugar, el mero hecho de que la difusión pueda perjudicar el interés nacional no significa que el daño sea mayor que los beneficios de la publicación; en segundo lugar, un "caso a caso" de equilibrio de daño versus beneficio, resultar difícil de manejar, es impredecible e impracticable; en tercer lugar, como hemos aprendido de nuestra propia historia, hay grandes presiones que conducen tanto a los funcionarios del gobierno y al propio público a subestimar los beneficios de la publicación y exagerar el daño potencial de la publicación en momentos de angustia nacional.

[754] Idem, p.114, referencia 26, citando el juicio *New York Times Co. vs. United States*, 403 U.S. 713 (1971).

[755] Esto puede parecer torpe, incluso incoherente: Si el gobierno puede prohibir constitucionalmente a los empleados públicos la revelación de información clasificada a los demás ¿por qué no puede imponérselo a los destinatarios? Se podría dar vuelta con la misma facilidad la pregunta: Si los individuos tienen un derecho a publicar información clasificada a menos que de la publicación "sin duda resultará un daño directo, inmediato e irreparable a nuestra nación y su gente", ¿por qué se le debe permitir al gobierno prohibir a sus empleados revelar dicha información a los demás simplemente porque representa un peligro potencial para la seguridad nacional? Si vemos el tema desde la perspectiva de cualquiera de los intereses del público en el discurso informado o el interés del gobierno en el secreto, parece que la misma regla lógica debería aplicarse tanto a los empleados públicos como a los que se les difundirá la información. Las grandes diferencias entre las normas que rigen a los empleados públicos, por una parte, y a otros oradores, por el otro, representa un misterio. Idem.

Una norma estricta de peligro claro y presente serviría como una barrera para protegernos contra este peligro; y en cuarto lugar, un principio central de la Primera Enmienda es que la supresión vía intervención pública debe ser el último recurso del gobierno para hacer frente a un problema potencial. Si hay otros medios por los cuales el gobierno puede prevenir o reducir el riesgo, se deben agotar otros medios antes de que se pueda suprimir la libertad de expresión. Esto, también, es una premisa esencial de la norma de peligro claro y presente. En la hipótesis de la clandestinidad, la manera más obvia en que el gobierno puede evitar el peligro es garantizando seriamente que la información perjudicial, en primer lugar, no se filtrará.[756]

La solución para él, es intentar conciliar los valores irreconciliables del secreto y la rendición de cuentas, garantizando tanto una fuerte autoridad para prohibir fugas al gobierno y un derecho amplio de otros para difundirlos.[757]

Tres preguntas permanecen. Primero ¿la misma norma constitucional regularía las restricciones previas y los procesos penales?; Segundo ¿qué tipo de revelaciones podrían satisfacer el estándar de peligro claro y presente?; Y tercero ¿cómo debemos tratar la información que satisface tanto el estándar de peligro claro y presente como el de contribuir significativamente al debate público?[758]

Para la primera pregunta, expone, en el caso de los Papeles del Pentágono, la Corte hizo hincapié en que se trata de un mandamiento judicial contra el discurso. Esta orden judicial habría sido la de una restricción previa, un tipo de restricción al discurso que, en palabras de la Corte, tiene una particular “presunción fuerte contra su constitucionalidad”. Plantea que en relación con la expresión en el corazón mismo de la Primera Enmienda - el

[756] Idem, p. 115.
[757] Idem, p. 116.
[758] Idem.

discurso sobre la conducta misma del gobierno - la distinción entre la restricción previa y el procesamiento criminal no debería ser de mucho peso. El criterio aplicado en los *Pentagon Papers* es esencialmente el mismo estándar que sería aplicable en un proceso penal de una organización o individuo que difunda públicamente información sobre la conducta del gobierno. El estándar peligro claro y presente, estima, no se ha limitado a los casos de censura previa.[759]

Para la segunda, los ejemplos ofrecidos tradicionalmente eran "las fechas de salida de los transportes" o la "ubicación de las tropas de combate", precisamente en tiempos de guerra. La publicación de esa información en ese instante hace que las tropas estadounidenses se vuelvan vulnerables a un ataque enemigo y frustre los planes de batalla ya en marcha. Otros ejemplos podrían incluir la publicación de la identidad de los agentes encubiertos de la CIA o la revelación pública de que el gobierno ha violado el código secreto de *al-Qaeda*, alertando así al enemigo a cambiar su sistema de cifrado. En situaciones como éstas, el daño de la publicación podría ser lo suficientemente probable, inminente y grave para justificar el castigo de la divulgación, estima.[760]

Para la tercera, dice, una característica importante de estos ejemplos a menudo pasa desapercibido. Lo que hace convincentes a estas situaciones no es sólo la posibilidad inminente y la magnitud de los daños, sino también el supuesto implícito de que este tipo de información no contribuye significativamente al debate público. En la mayoría de los casos, no hay una necesidad evidente de que el público conozca el secreto de las "fechas de salida de los transportes" o el secreto de la "ubicación de las tropas estadounidenses" en la víspera de la batalla. En ese instante estas cuestiones son irrelevantes para la discusión política. Después del hecho, argumenta, por

[759] Idem
[760] Idem.

supuesto que esa información puede ser crítica para la evaluación de la efectividad de nuestros líderes militares, pero en el mismo momento en que los barcos se ponen a navegar o que las tropas se ponen a atacar, no está tan claro lo que aporte esa información al debate público. Su punto, expresa, no es que estos ejemplos impliquen expresiones de "bajo" valor en el sentido convencional del término, sino que implican que la información no parece especialmente "de interés periodístico o noticioso" en el momento de la publicación.[761]

Sugiere suponer por ejemplo, que un periódico informa con exactitud que las tropas estadounidenses en Afganistán asesinan recientemente a veinte miembros de *al-Qaeda* a sangre fría. Como resultado de esta publicación, *al-Qaeda* secuestra y asesina veinte ciudadanos estadounidenses. ¿Puede el periódico constitucionalmente ser castigado por la divulgación de la masacre inicial? La respuesta, piensa, debe ser no. Incluso, dice, existiendo un peligro claro y presente de que una represalia pueda sobrevenir, e incluso si estamos de acuerdo en que se trataría de un grave daño, la información es demasiado importante para el pueblo estadounidense como para castigar su divulgación.[762]

Lo que propone el profesor Stone, es que para justificar la sanción penal de la prensa por la publicación de información clasificada, el gobierno debe demostrar no sólo que el demandado publicó información clasificada, cuya publicación podría resultar en un daño probable, inminente y grave para la seguridad nacional, sino que también deberá demostrar que la publicación no contribuiría significativamente al debate público.[763]

III.4.3.3.c. Posición del profesor Benkler. A propósito del peligro claro y presente que tendría que demostrarse para restringir la expresión en interés de

[761] Idem, p. 117.
[762] Idem.
[763] Idem.

la seguridad nacional, plantea que la larga historia desde el caso *Schenck v. United States (1919)*, *Whitney v. California (1927), Brandenburg v. Ohio (1969)*, para abrazar el estándar de "peligro claro y presente" terminó requiriendo una combinación similar de alta probabilidad, de alto daño y de la inmediatez del proceso. Cuando la Corte Suprema se puso en el contexto de considerar la responsabilidad penal de un locutor que había transmitido materiales ilegales, estimó que la Primera Enmienda no permite el enjuiciamiento de un periodista que transmite información veraz de interés público "en ausencia de una necesidad de primer orden"[764]. Por lo tanto, el estándar para la censura previa y el de la persecución penal por la publicación de materiales veraces de interés público parece ser básicamente el mismo, y sumamente estricto[765]-[766].

III.4.3.3.d. Posición del abogado Elsea del CRS. Expone que cuando se trata de limitar el habla en función de su contenido la Corte Suprema aplica en general un "estricto escrutinio", lo que significa que va a defender una restricción basada en el contenido sólo si es necesario para "promover un interés apremiante", y es "el medio menos restrictivo para promover el interés articulado" [767]. La protección de la seguridad nacional ante amenazas externas es, sin duda, un interés gubernamental apremiante[768]. Durante mucho tiempo se ha aceptado que el gobierno tendría una necesidad imperiosa de suprimir ciertos tipos de discurso, sobre todo en tiempos de guerra o de riesgo elevado

[764] BENKLER, op. cit., p. 35, referencia 210 citando a *Bartnicki vs. Vopper* 532 U.S. 514, 528 (2001) (citando a su vez a *Smith vs. Daily Mail Publishing Co*., 443 U.S. 97, 103 (1979)).
[765] Idem, p. 35, referencia 211.
[766] "En el trasfondo de esta barrera extremadamente alta para ambos, censura previa y enjuiciamiento criminal, tal vez no sea sorprendente que los esfuerzos de la Administración Bush para enjuiciar al *New York Times* por sus revelaciones sobre el programa de la Agencia de Seguridad Nacional de espionaje interno, y al *Washington Post* por la presentación de informes sobre la existencia de sitios operados por la CIA en Europa del Este, fueron abandonados." Idem, referencia 212.
[767] ELSEA, op. cit., p.21, referencia 130, citando a su vez *Sable Communications of California v. Federal Communications Commission*, 492 U.S. 115, 126 (1989).
[768] Idem.

de hostilidades[769]. Discursos susceptibles de incitar a la violencia inmediata, por ejemplo, también pueden ser suprimidos[770]. El discurso que daría ventaja militar al enemigo extranjero también sería susceptible de regulación gubernamental.[771]

Se pregunta ¿Qué derechos de la Primera enmienda están implicados? Argumenta que si el gobierno tiene una necesidad imperiosa de sancionar la divulgación de información clasificada, se activa si la divulgación tiene el potencial de causar daños a la defensa nacional o a las relaciones exteriores de los Estados Unidos. Los daños reales, dice, no necesitan ser probados, pero el daño potencial debe ser más que meramente especulativo e incidental. Por otra parte, la Corte ha dicho que:

"la acción del Estado para castigar la publicación de información veraz rara vez cumple las normas constitucionales"[772].

Y se ha descrito el propósito detrás de la garantía constitucional de la libertad de prensa como la protección de "la libre discusión de los asuntos gubernamentales"[773].

Aunque la información debidamente clasificada, plantea, de ser revelada a una persona no autorizada para recibirla es identificable como potencial para causar daño a la seguridad nacional de los Estados Unidos[774], no se desprende

[769] Idem, p.22, referencia 132, citando a su vez *Schenck v. United States*, 249 U.S. 47 (1919) (formulando el test de "peligro claro y presente").
[770] Idem, referencia 133, citando a su vez *Brandenburg v. Ohio*, 395 U.S. 444 (1969).
[771] Idem, referencia 134, citando a su vez *Near v. Minnesota*, 283 U.S. 697, 716 (1931) ("Nadie duda de que un gobierno puede evitar la obstrucción real a su servicio de reclutamiento o de la publicación de las fechas de salida de los transportes o el número y la ubicación de las tropas".).
[772] Idem, referencia 137, citando a su vez *Bartnicki vs. Vopper*, 532 U.S. 514, 527 (2001) (citando a *Smith v. Daily Mail Publishing Co*., 443 U.S. 97 (1979)).
[773] Idem, referencia 138, citando a su vez *Mills v. Alabama*, 384 U.S. 214, 218 (1966). Puesto que el objetivo de la Primera Enmienda es proteger la capacidad del público para discutir asuntos de gobierno junto con las decisiones judiciales que nieguen proporcionar ningún derecho especial a los periodistas.
[774] Idem, p.23, referencia 139, citando a su vez Exec. Order No. 13526, 75 Fed. Reg. 707 §1.2 (January 5, 2010) ("Classified National Security Information").
Section 1.3 define tres niveles de clasificación:

necesariamente que la clasificación del gobierno por sí sola sea determinante de la cuestión en el contexto de un proceso penal. Sin embargo, dice, los tribunales han adoptado como elemento de los estatutos de espionaje el requisito de que la información en cuestión debe ser "mantenida estrechamente"[775]. Si bien la clasificación del gobierno sería una fuerte evidencia para apoyar esta afirmación, los jueces han reconocido que el gobierno debe demostrar que la divulgación de información específica de la defensa nacional tenga el potencial de dañar los intereses estadounidenses, pues de otra manera, la Ley de Espionaje sería un medio para castigar a los denunciantes que revelen información embarazosa para los funcionarios públicos más que para castigar la puesta en peligro de la seguridad nacional.[776]

(1) "Top Secret" se aplicará a la información, de la que podría esperarse razonablemente que su divulgación no autorizada pueda causar daño excepcionalmente grave a la seguridad nacional, que la autoridad de clasificación original es capaz de identificar o describir.
(2) "Secreto" se aplicará a la información, de la que podría esperarse razonablemente que su divulgación no autorizada pueda causar un perjuicio grave a la seguridad nacional, que la autoridad de clasificación original es capaz de identificar o describir.
(3) "Confidencial" se aplicará a la información, de la que podría esperarse razonablemente que la divulgación no autorizada pueda causar daño a la seguridad nacional que la autoridad de clasificación original es capaz de identificar o describir.

[775] Idem, referencia 140 citando a su vez *United States v. Heine*, 151 F.2d 813 (2d Cir.1945) la información debe ser "estrechamente sostenida" para considerarse "en relación con la defensa nacional" en el sentido de las leyes de espionaje.

[776] Idem, p. 23.

TOMA DE POSICIÓN

Respecto a la posibilidad de procesar a Julian Assange según la *Espionage Act*, concuerdo con el profesor Barron en lo términos de afirmar también que la misma constitucionalidad de la ley de espionaje podría discutirse. La vaguedad de sus términos y obsolescencia claman por una regulación acorde con los estándares de la primera enmienda. La decisión del juez Ellis en el caso *AIPAC* de aceptar la tramitación del caso según la Ley de Espionaje pero establecer el requisito de la necesidad de probar la intención específica de generar daño es un hecho sustancial para justificar nuestra aceveración anterior. Este requisito, además, sería muy difícil de cumplir, dando cuenta de las notas enviadas por Assange para solicitar información al gobierno acerca de lo considerado por este último como un actuar responsable en estas circunstancias, y teniendo en cuenta también, la sabida colaboración preventiva del *The New York Times* hacia el mismo gobierno. Esto implica que, además de la demostración de una intención no dañosa o de por lo menos hacer muy compleja la prueba de una intención dañosa, el hecho de que se previno al gobierno para que este último ganara tiempo, se preparara y pudiera administrar sus esfuerzos de mejor manera que lo que podría haber hecho ante una circunstancia pura y simplemente sorpresiva, típicamente dañosa y que profita de la vulnerabilidad en que se sitúa a la contraparte ante un evento de naturaleza intempestiva.

Por el mismo motivo también estamos de acuerdo con Jones y Ward en la importancia de que Assange haya escrito al gobierno pidiendo sugerencias para las redacciones haciendo muy complejo probar que actuó con mala intención.

Respecto a la opinión de Elsea en este contexto concordamos a propósito de la necesidad de probar la mala intención y en el interesante aporte

de agregar la posición interpretativa de la sección 793 que excluye de posibles sanciones a la publicación de material clasificado.

Compartimos también con Barron el punto de que aun ante la improbable circunstancia de probarse la intención específica, para condenar a Assange esta posibilidad debe superar su contraste con la primera enmienda.

Todo lo anterior también en la misma línea de lo planteado por el profesor Shoenfeld en relación a que la ley de Espionaje es equívoca y podría plantear grandes problemas de constitucionalidad y por el profesor Carter que plantea que el discurso o la libertad de expresión jamás debería asociarse a un contexto en el que pudiese ser aplicable una sanción penal.

Siendo nuestra posición la de una más que improbable posibilidad de demostración de una mala intención de Assange, de todas maneras consideramos analizar si la aplicación de una sanción sería constitucional o no.

En este punto, con respecto a si *WikiLeaks* es o no parte de la prensa y concordamos con lo opinado por el profesor Barron en relación a que no podríamos excluir a *WikiLeaks* de la protección a la libertad de prensa por transmitir su contenido a través de Internet en lugar de a través de páginas impresas, sobretodo porque justamente medios tradicionales han trabajado coordinadamente con *WikiLeaks*, siendo que ni el *Washington Post* ni el *The New York Times* están siendo perseguidos penalmente.

Coincidimos con el profesor Benkler en que la diferencia entre los medios tradicionales y aquellos nacidos de la cultura descentralizada de la Internet es meramente organizativa. Diferencia que no sostiene una distinción que implique diferencias en su protección constitucional. Es más, justamente es más importante aclarar que los miembros más débiles de la Internet, sin recursos para resistir las presiones de los gobiernos, deben ser protegidos

constitucionalmente. Cita plausiblemente también el caso *Von Bulow vs. Von Bulow (2nd Cir. 1987)*, en que el tribunal destacó que ser un periodista establecido no es necesario para la protección.

Sostenemos al igual que Benkler que el elemento definitorio fundamental es la intención en el momento de la recolección y su función, no el modo de difusión. Además, en que no es relevante si su interés fue o no perjudicar al gobierno estadounidense. También, en que la primera enmienda niega privilegiar al *New York Times* por sobre *WikiLeaks* debido a su funcionamiento interno, pues la esfera de lo público se ha diversificado en la red, siendo urgente separarse de una interpretación judicial que se limite a proteger a los grandes medios del siglo XX.

Finalmente coincidimos también en que un enjuiciamiento contra Assange o *WikiLeaks* seguramente no prosperaría.

Tomamos posición también desde lo dicho por Jones y Ward en relación a que es difícil argumentar que *WikiLeaks* no realiza ninguna función periodística tradicional, pues cabalmente entendida, la Primera Enmienda no se preocupa si *WikiLeaks* es un acreditado distribuidor de noticias, un grupo de *hackers* o un circo ambulante precisamente porque la protección que ésta ofrece depende de lo que WikiLeaks publica, no de lo que es.

Concordamos en la importancia de subrayar el principio Daily Mail generado por la Corte Suprema en 1979 que establece que:

“la información veraz sobre un asunto de interés público” recibe muy amplia protección ante la responsabilidad penal o civil.

Y que ha sido desarrollado en *Bartnicki vs. Vopper recientemente en 2001* describiéndose que cuando la discusión se fundamenta sobre información veraz acerca de un asunto de importancia pública, la Corte reafirmó:

“entonces los funcionarios del Estado no pueden castigar constitucionalmente la publicación de la información, en ausencia de una necesidad… de primer orden”.

La Corte también hizo hincapié en que el grado de protección que ofrece la Primera Enmienda no varía en base a la identidad del hablante o la percepción de la utilidad social de la información difundida. Además, refiriéndose a la circunstancia en la que el editor obtiene la información sabiendo que la fuente ha actuado ilegalmente en la obtención o diseminación, el Tribunal directamente sostuvo que “la conducta ilegal de un extranjero no es suficiente para eliminar la protección de la Primera Enmienda al debate sobre un asunto de interés público”.

En el mismo sentido rescatamos lo opinado por Elsea, abogado del Servicio de Investigación del Congreso, de que no es casualidad que el Tribunal Supremo no haya establecido límites claros entre la protección de la expresión y de la prensa, ni haya tratado de desarrollar criterios para determinar lo que constituye “la prensa”, para poder calificar a sus miembros con privilegios que no estén disponibles para cualquier persona.

A propósito de la pregunta de quién sería el garante de que los secretos del gobierno sigan siéndolo, coincidimos con Benkler en que *WikiLeaks* en ningún caso tiene que cumplir con el rol de cuidar que los secretos del gobierno no sean conocidos. Citamos también los *Pentagon Papers* en relación a que el ejecutivo tiene la responsabilidad de mantener sus propias operaciones con suficiente seguridad y sabiduría para asegurarse de que sólo lo que necesita clasificar es de hecho clasificado, y lo que se clasifica no consiga ser filtrado.

Coherente con ello tomamos la posición de Posner de rechazar la clasificación excesiva de información y documentos porque hace que los esfuerzos por protegerlos sean ridículos.

Con Schoenfeld convergemos en que el secreto podría ser utilizado para cubrir la corrupción y el delito, por lo que dependemos de la libertad de prensa para que se nos proporcione información acerca de lo que el gobierno está haciendo en representación nuestra, incluyendo algunas de las cosas que están en secreto. La publicación periódica de los secretos es parte del sistema estadounidense, y esa es la manera en que debe ser.

De esta manera, por supuesto que los periodistas no deben ser procesados siempre que publiquen un secreto, sino que sólo cuando ponen al país en peligro.

En lo que diferimos con el es que si bien también entendemos que ciertos documentos al publicarse claramente ayudan a entender mejor el papel de EE.UU. y otros generan daño ello de ninguna manera es concluyente para sancionar la conducta pues queda por probar si hubo intención precisa y directa en esa dirección y no sólo la intención de informar y develar situaciones de delito y hasta de crímenes llevados a cabo por el ejército estadounidense.

Acerca de la pregunta de si se expuso intencionalmente la seguridad nacional de EE.UU. concordamos plenamente con la postura del profesor Stone a propósito de las razones que fundamentan la actitud de los gobiernos ante el secreto, que va desde el resguardo a la seguridad nacional hasta el ocultamiento de incompetencias e incluso crímenes, como es en este caso de estudio.

El verdadero dilema no está presente cuando se divulga información clasificada que puede ser muy valiosa para el debate público, como el uso secreto de interrogatorios coercitivos o la autorización secreta de vigilancia electrónica generalizada. El verdadero dilema, coincidimos con Stone, surge cuando la divulgación pública de información secreta es tanto perjudicial para la seguridad nacional, como valiosa para el debate público.

Es de importancia determinante subrayar que nunca en este contexto ha existido un procesamiento exitoso, la Corte Suprema nunca ha tenido ocasión de pronunciarse sobre este tipo de caso. Lo más cerca que ha llegado a tal situación fue en los *Pentagon Papers*, resolviéndose inconstitucional el intento del gobierno de prohibir la publicación. La opinión del juez Stewart capta la opinión de la Corte: "(…) Estoy convencido de que el Ejecutivo tiene razón con respecto a algunos de los documentos en cuestión. Pero no puedo decir que la divulgación de cualquiera de ellos seguramente resultará en un daño directo, inmediato e irreparable a nuestra nación o a su gente". Así, aunque el ejecutivo tiene amplia autoridad para mantener la información en secreto clasificado, una vez que la información llega a otras manos sólo tiene una autoridad limitada para evitar su ulterior difusión.

Coincidimos en que la solución es intentar conciliar los valores opuestos del secreto y de la rendición de cuentas, garantizando tanto una fuerte autoridad del gobierno para prohibir fugas y un derecho amplio de los demás para difundirlos.

Creemos también que el criterio aplicado en los *Pentagon Papers* es esencialmente el mismo estándar que sería aplicable en un proceso penal contra una organización o individuo que difunda públicamente información sobre la conducta del gobierno. El estándar peligro claro y presente no se ha limitado a los casos de censura previa.

También en que para entender que la publicación hace daño ella debe poner en una situación de vulnerabilidad temporalmente insuperable al gobierno y que ello ponga en peligro claro y presente al país y que por ejemplo, si un periódico informa que las tropas en Afganistán asesinan a veinte miembros de *al-Qaeda* a sangre fría y como resultado de esta publicación, *al-Qaeda* secuestra y asesina veinte ciudadanos estadounidenses, el periódico no debe

ser castigado. Pues aun existiendo un peligro claro y presente de represalia, incluso estando de acuerdo en que se trataría de un grave daño, la información es demasiado importante para el pueblo como para castigar su divulgación.

El gobierno deberá entonces demostrar, no sólo que el demandado publicó información clasificada, cuya publicación podría resultar en un daño probable, inminente y grave para la seguridad nacional, sino que también deberá demostrar que la publicación no contribuiría significativamente al debate público.

Del mismo modo, coincidimos con Elsea en que los daños reales, dice, no necesitan ser probados, pero el daño potencial debe ser más que meramente especulativo e incidental.

CONCLUSIONES

Primero que todo y haciéndonos cargo de la pregunta del párrafo III.4.1. podemos afirmar que los actos de *WikiLeaks* no son ciberterrorismo simplemente porque en nuestro concepto ni siquiera aun ha acaecido el primer acto ciberterrorista de la historia.

Tampoco sus actos son *hacking* (ni *hacktivismo* en sus actividades asimilables al *hacking*) en su acepción negativa que es la que está incluída en las conductas de delincuencia informática, ya que según los antecedentes que existen ni Julian Assange ni *WikiLeaks* han accedido ilegalmente a los sistemas de información o a las redes de computadores norteamericanos, sino que los documentos fueron facilitados “desde adentro” por el soldado Manning, y en la peor de las hipótesis, habrían sido obtenidos a través del sistema Tor, pero que no corresponde a una red informática estadounidense, sino que se trata de una red de unos 2.000 servidores informáticos globales y voluntarios.

Las actividades de *WikiLeaks* ni siquiera encuadran dentro de lo que entendemos por *hacktivismo* en su matiz más benévola, pues no se han dedicado ni siquiera a efectuar las inofensivas desfiguraciones de sitio para activar sus ideas de cambio social y político.

Evidentemente con todos estos antecedentes la *Computer Fraud and Abuse Act* es inaplicable a Julian Assange, dado que no ha existido acceso no autorizado a computadores o redes de computadores del gobierno estadounidense. Tampoco podría hablarse de complicidad o encubrimiento, dado que ni siquiera *WikiLeaks* podía acceder a la identidad de sus fuentes en su sistema ideado para protegerlas.

Estimamos que la ley de espionaje tampoco es aplicable a las conductas de *WikiLeaks*, pensamos que al recibirse u obtenerse la información no se tuvo

intención de lesionar a Estados Unidos ni que la obtención de ella fue motivada para provocarle daño; tampoco, que al poseerse sin autorización documentos de la defensa de EE.UU. y comunicarse voluntariamente a quien no tenía derecho a recibirla se tuvo la intención de dañarlo. Estimamos que no se podrá probar ni la intención específica de daño ni el daño potencial a la seguridad nacional:

En lo referido a la prueba de la intención específica, fue la decisión en *Hartzel v. Estados Unidos (1944)* la que esbozó el criterio estándar de un procesamiento exitoso: "salvo que se encuentren pruebas suficientes de que un jurado pudiese inferir más allá de una duda razonable de que tenía la intención de llevar a cabo las consecuencias específicas prohibidas por la ley (…)" la libertad de expresión y de prensa están protegidas. Ello fue reforzado por el juez del caso *AIPAC* que estableció que un enjuiciamiento exitoso debe probar que el acusado sabe que la divulgación de la información de defensa es perjudicial para Estados Unidos y lo hace con intención de que ese daño se materialice.

No se podrá probar, porque al recibirse u obtenerse los documentos no se sabía qué se obtenía ni desde dónde, siendo la intención aplicable en este contexto la intención genérica del sitio *WikiLeaks*, el de recibir documentos en que se contenga información de posibles malas prácticas de gobiernos o de empresas, no la de hacer daño a los Estados Unidos, lo que a mayor abundamiento se prueba por las primeras filtraciones llevadas a cabo por el sitio las que motivaron incluso un premio de Amnistía Internacional y, además, porque no tenía conocimiento de su fuente.

Tampoco podrá probarse o se hace aun más complejo probar la intención dañosa en la segunda hipótesis en relación a la posesión y comunicación del material, pues, agregando los argumentos anteriores,

debemos hacer mención a las peticiones enviadas por Julian Assange, incluso desde los diarios de guerra de Afganistán, al gobierno norteamericano a través de *The New York Times,* solicitando información acerca del estándar en que una publicación podría constituir una amenaza para las personas, las cuales no fueron respondidas en abstracto, pero tampoco en concreto existiendo esta posibilidad, pues el *New York Times* enviaba a su gobierno cierta cantidad de documentos a modo de alerta temprana antes de cada publicación. Por lo tanto había una intención de prevenir cualquier tipo de daño y un conocimiento previo de lo que se publicaría por parte del eventual afectado.

A ello hay que agregar que en el fallo sobre el caso papeles del pentágono un juez de la mayoría declaró que a propósito de la expresión "comunica" de la ley ello no puede identificarse a la expresión "publica", por lo que la publicación de la información no sería una conducta reprochada. Además, a mayor abundamiento y en concordancia con la doctrina de la Primera Enmienda expuesta durante el transcurso de este trabajo, resultaría por decirlo menos forzado argumentar que el pueblo estadounidense no tuviese derecho a recibir la información, sobretodo de actuaciones ilícitas de quienes los representan y deciden el destino de la nación, como crímenes de guerra, violaciones a los derechos humanos y espionaje internacional.

Debemos también destacar que la única ocasión en que se invocó directamente contra la prensa no surgió en un proceso penal, sino que en los "*Pentagon Papers*" y estamos de acuerdo con el profesor Barron en que al establecerse sus disposiciones desde un lenguaje vago y demasiado amplio se podrían plantear cuestiones de constitucionalidad de la ley.

Finalmente es de interés además agregar la opinión de Jones y Ward en relación a que si hubiese sido un *mass media* el acusado*,* respondería alegando que su intención era la de informar sobre asuntos pertinentes al *self-*

government, que no se violó la ley ni se dañó al gobierno y así se ha interpretado la intención por los tribunales en circunstancias análogas. Es interesante porque entrega un argumento a la defensa entendiendo que operaría de manera excluyente en favor de la prensa. ¿Y cómo cumplir con el concepto de prensa? ¿Es determinante?

Estimamos que el hecho de que *WikiLeaks* sea o no parte de la prensa no es relevante para solicitar la protección de la primera enmienda. Concordamos con el profesor Benkler en el sentido de que la protección de la primera enmienda más que al aparato formal que realiza la publicación está dirigida a tutelar el punto de si de lo que trata la información resulta relevante para el debate de la comunidad nacional representada, dada la configuración de realidad necesaria para tomar decisiones colectivas para validar o sustituir a sus propios representantes y en términos más amplios incluso validando y profundizando la misma democracia.

A mayor abundamiento, pensamos que la descontrolada inflación, sobretodo en los últimos años, de la información categorizada como clasificada, desnaturaliza la relación que se supone existente entre su revelación no autorizada y un daño a la seguridad nacional. De hecho, incluso luego de una de las publicaciones el mismo gobierno de Estados Unidos recalificó al material disminuyendo su calificación, su protección y en definitiva su relación con un daño a la seguridad nacional. Establecido ello por la doctrina, pierde poder el argumento relativo a que una información clasificada revelada sea *per se* daño o puesta en peligro de la seguridad nacional norteamericana.

Establecido lo anterior tendríamos que recurrir a la doctrina del peligro claro y presente. Estimamos que de aplicarse aquella doctrina a las revelaciones de *WikiLeaks* en estos momentos y aun más en el futuro ya resulta evidente que no hubo peligro claro y presente a la seguridad nacional

estadounidense pues de los antecedentes ofrecidos en este trabajo se dejó en claro que no se pudo demostrar que una sola persona ligada a la seguridad nacional estadounidense haya muerto debido a las filtraciones y que incluso habiendo ocurrido ello, que no ocurrió, tampoco implicaría un riesgo de la entidad requerida por la doctrina para entender que la nación estadounidense se encontró en peligro. A mayor añadidura y entendiendo que no sería aplicable al caso *WikiLeaks* estimamos que en el futuro simplemente aquella doctrina no se debe aplicar debido a la imprevisibilidad y abuso del que dejamos testimonio, inadmisible para la claridad de redacción de la primera enmienda y un desarrollo coherente de ella, ni siquiera pensando en el futuro sino que en una visión tenida por un juez supremo de la república estadounidense en 1969.

BIBLIOGRAFÍA

Libros

DOMSCHEIT-BERG, Daniel, *"Inside WikiLeaks"*. Traducido por Ana Duque de Vega y Carles Anfreu Saburit bajo el título *"Dentro de Wikileaks. Mi etapa en la web más peligrosa del mundo"*, Rocaeditorial, 2011.

LEIGH, David y Harding, Luke. *"Wikileaks: Inside Julian Assange´s War on Secrecy"*, Guardian books, traducción de Mar Vidal e Isabel Merino bajo el título: *"Wikileaks y Assange. Un relato trepidante sobre cómo se fraguó la mayor filtración de la historia"*, Ediciones Deusto, Barcelona, 2011.

O´HAGAN, Andrew. *"Julian Assange. The Unauthorised Autobiography*", Cannongate books, traducción de Enrique Murillo para Los libros del Lince/Catalonia bajo el título *"Julián Assange. La verdad amordazada. Autobiografía no autorizada."*, Santiago de Chile, 2012.

Revistas especializadas

AMERICAN ACADEMY OF ARTS & SCIENCES*, "WikiLeaks & the First Amendment"*, Bulletin of the American Academy of Arts & Sciences, Spring 2012.

AMMORI, Marvin. "*First Amendment Architecture*", Stanford Law School - Center for Internet & Society; New America Foundation - Open Technology Initiative, 11 de Marzo de 2011, Wisconsin Law Review, Vol. 2012, No. 1, 2012.

BARRON, Jerome A., *"The Pentagon Papers case and the WikiLeaks controversy: National Securiry and the First Amendment"*, Wake Forest Journal of Law & Policy, Vol 1:1 2011.

BENKLER, Yochai. *"A free irresponsible press: Wikileaks and the battle over the soul of the networked fourth estate"*. Harvard Civil Rights-Civil Liberties Law Review, 2011.

CARR Wilfred, Kemmis Stephen. *"Teoría crítica de la enseñanza"*. La investigación-acción en la formación del profesorado. 1986. Martínez Roca, Barcelona. Cap. 5 pp. 140-166

CEBRIÁN, Mariano. *"La Web 2.0 como red social de comunicación e información"*, Estudios sobre el Mensaje Periodístico, 2008, 14, p. 345-361, [en línea] <http://www.ucm.es/info/emp/Numer_14/Sum/4-04.pdf>

CLOUGH, Jonathan. *"Data theft? Cybercrime and the increasing criminalization of acces to data"*, Criminal Law Forum (2011) 22:145–170.

DAUGHERTY, Terry, Eastin, Matthew S., Bright, Laura F. y Chu, Shu-Chuan. Chapter 7 Expectancy-Value: *"Identifying Relationships Associated with Consuming User-Generated Content"*. En: EASTIN, Matthew S., DAUGHERTY, Terry y Burns, Neil M., *"Handbook of Research on Digital Media and Advertising: User Generated Content Consumption"*. Information Science Reference, 2011.

DENNING, Dorothy E. "*Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy"*, [en línea] <http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf>

DENNING, Dorothy E. *"CYBERTERRORISM"*, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives by Georgetown University, May 23, 2000, [en línea] <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>

EBERSBACH, Anja y Glaser, Markus. *"Towards Emancipatory Use of a Medium: The Wiki"*. International Journal of Information Ethics, Vol. 2 (11/2004) [en línea] <http://fiz1.fh-potsdam.de/volltext/ijie/05250.pdf>

ELSEA, Jennifer K., *"Criminal prohibitions on the publication of classified defense information"*, Congressional Research Service, 31 de enero de 2013.

EMERSON, Thomas I. *"The doctrine of prior restraint"*, 1955, Yale Law School Legal Scholarship Repository.

HALL, Wendy. *"The Ever Evolving Web: The Power of Networks"*. International Journal of Communication 5, 2011, p. 655. [en línea] <http://eprints.soton.ac.uk/272374/1/evolvingwebfinal.pdf>

HAMPSON, Noah C.N., *"Hacktivism: A new breed of protest in a networked world"*, Boston College International and Comparative Law Review [Vol. 35:511 2012].

KRASAVIN, Serge. *"What is Cyber-terrorism?",* Computer Crime Research Center, July 2000, [en línea] <http://www.crime-research.org/library/Cyber-terrorism.htm>

LAMB, Brian. *"Wide Open Spaces: Wikis, Ready or Not"***.** Educause Review*,* vol. 39, no. 5 (September/October 2004): 36–48. [en línea] <www.educause.edu/ero/article/wide-open-spaces-wikis-ready-or-not>

JONES, Shaina y Ward Brown, Jay,*"The Assange Effect: WikiLeaks, the Espionage Act and the Fourth Estate",* En: Media Law Resource Center Bulletin, August, 2011.

MAGALLÓN, Raúl*. "Wikileaks: ¿Un cambio de paradigma?"*. *Estudios sobre el mensaje periodístico.* Vol. 18, núm. 1, 2012, págs.: 127-132. Madrid, Servicio de Publicaciones de la Universidad Complutense.

MCQUADE, Samuel, *"Encyclopedia of cybercrime"*, Greenwood Publishing Group, 2009.

MAURER, Tim, *"WikiLeaks 2010: A Glimpse of the Future?"*. Discussion Paper 2011-10, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, August 2011, p.7. [en línea] <http://belfercenter.ksg.harvard.edu/files/maurer-dp-2011-10-wikileaks-final.pdf>

QUESADA, Rocío. *"La didáctica crítica y la tecnología educativa"* Revista Perfiles Educativos de la Universidad Nacional Autónoma de México, No. 49 – 50 pp. 3 – 13. 1990. [en línea] <http://132.248.192.201/seccion/perfiles/1990/n49-50a1990/mx.peredu.1990.n49-50.p3-13.pdf>

SANCHEZ, Carlos. *"Analogías de la Historia I: Julian Assange y Wikileaks vs Daniel Ellsberg y los Pentagon Papers"*. Nómadas. Revista Crítica de Ciencias Sociales y Jurídicas de la Universidad Complutense de Madrid. No. 31, 2011, p.11. [en línea] <http://www.redalyc.org/redalyc/pdf/181/18120621004.pdf>

SANCHEZ, Gema. *"Cibercrimen, ciberterrorismo y ciberguerra: Los nuevos desafíos del s. XXI"*, Revista Cenipec, 31, 2012.

STONE, Geoffrey, *"WikiLeaks, the Proposed SHIELD Act, and the First Amendment"*, Journal of National Security Law & Policy, [Vol. 5:105 2011].

U.S. GOVERNMENT PRINTED OFFICE (GPO), *"First amendment. Religion and Expression"*, [en línea] < http://www.gpo.gov/fdsys/pkg/GPO-CONAN-2002/pdf/GPO-CONAN-2002-9-2.pdf>

Artículos de Prensa

ABC, “Assange confirma que presentará su candidatura al Senado australiano en 2013”. 14 de diciembre de 2012. [en línea] <http://www.abc.es/internacional/20121213/abci-assange-candidatura-senado-australiano-201212130235.html>

DER SPIEGEL*, “Old Wars and New: Estonians Accuse Kremlin of Cyberwarfare”*, 17 de mayo de 2007, [en línea] <http://www.spiegel.de/international/world/old-wars-and-new-estonians-accuse-kremlin-of-cyberwarfare-a-483394.html>

REUTERS, *“Wiki wins a place in Oxford English Dictionary”*, 15 de Marzo de 2007, [en línea] <http://www.reuters.com/article/2007/03/15/us-britain-dictionary-wiki-idUSL1528182320070315>

EL IMPARCIAL, *“Caso Assange: La solución Gambier:”*, 3 de Octubre de 2012, [en línea] <http://www.elimparcial.es/mundo/caso-assange-la-solucion-gambier-112077.html>

EL PAÍS. *“John Young, Un indiscreto en la web”*, 13 de Agosto de 2000. [en línea] <http://elpais.com/diario/2000/08/13/sociedad/966117603_850215.html>

EL PAÍS. *“Hackers chinos atacan la red militar de occidente”*. 16 de septiembre de 2010. [en línea] <http://elpais.com/diario/2007/09/16/internacional/1189893604_850215.html>

EL PAÍS. “Cita secreta con el hombre que hace temblar al Pentágono”. 24 de Octubre de 2010. [en línea] <http://elpais.com/diario/2010/10/24/domingo/1287892353_850215.html>

EL PAIS, “Clinton tacha la filtración de “robo” y ataque a la comunidad internacional”, 30 de noviembre de 2010; [en línea] <http://elpais.com/diario/2010/11/30/internacional/1291071608_850215.html>

EL PAIS, *“Enterrando al soldado Manning”.* Madrid, 20 de marzo de 2011. [en línea] <http://elpais.com/diario/2011/03/20/domingo/1300596753_850215.html>

EL PAÍS. *"Guantánamo como telón de fondo"*, 3 de Mayo de 2011. [en línea] <http://internacional.elpais.com/internacional/2011/05/03/actualidad/1304373617_850215.html>

EL PAÍS, *"WikiLeaks anuncia la publicación de todos sus cables sin ocultar sus fuentes"*, 3 de septiembre de 2011, [en línea] <http://elpais.com/diario/2011/09/03/internacional/1315000809_850215.html>

EL PAÍS. *"Por qué abandoné Wikileaks"*. 4 de Septiembre de 2011. [en línea] <http://elpais.com/diario/2011/09/04/internacional/1315087207_850215.html>

EL PAIS, "*Un tribunal de Londres aprueba la extradición de Julian Assange a Suecia"*, 2 de noviembre de 2011; [en línea] <http://internacional.elpais.com/internacional/2011/11/02/actualidad/1320221857_945649.html>

EL PAIS, *"La Corte Suprema británica rechaza el recurso de Julian Assange"*, 14 de junio de 2012, [en línea] <http://internacional.elpais.com/internacional/2012/06/14/actualidad/1339682033_882446.html>

THE GUARDIAN. "*The looting of Kenya"*, 31 de Agosto de 2007. [en línea] <http://www.guardian.co.uk/world/2007/aug/31/kenya.topstories3?INTCMP=SRCH>

THE GUARDIAN. *"Microsoft backs down over online spy guide"*. 25 de Febrero de 2010. [en línea] <http://www.guardian.co.uk/technology/blog/2010/feb/25/microsoft-cryptome-surveillance>

THE GUARDIAN, *"Julian Assange: the teen hacker who became insurgent in information war".* 30 de enero de 2011. [en línea] <http://www.guardian.co.uk/media/2011/jan/30/julian-assange-wikileaks-profile>

THE GUARDIAN, *"Bradley Manning: a sentence both unjust and unfair"*, 21 de agosto de 2013 [en línea] <http://www.theguardian.com/commentisfree/2013/aug/21/bradley-manning-sentence-unjust>

Comunicados de Prensa

BOTERO y La Rue, *"Declaración conjunta sobre WikiLeaks"*, [en línea] <http://www.oas.org/es/cidh/expresion/showarticle.as p?artID=829&lID=2>

Paginas Web

<c2.com/cgi/wiki?WikiWikiWeb>

<wikipedia.org/>

<http://oxforddictionaries.comi>

<http://www.rand.org>

< http://cryptome.org >

WIKILEAKS. "Union of Islamic Courts". [en línea] <http://www.wikileaks.org/wiki/Union_of_islamic_courts.zip>

WIKILEAKS, *"Camp Delta Standard Operating Procedure"*. [en línea] <http://wikileaks.org/wiki/ Camp_Delta_ Standard_Operating_Procedure >

WIKILEAKS, *"Bank Julius Baer"*. [en línea] < http://www.wikileaks.org/wiki/Bank_Julius_Baer >

WIKILEAKS, *"Financial collapse: Confidential exposure analysis of 205 companies each owing above EUR45M to Icelandic bank Kaupthing, 26 Sep 2008"*. [en línea] <https://www.wikileaks.org/wiki/Financial_collapse:_Confidential_exposure_analysis_of_205_companies_each_owing_above_EUR45M_to_Icelandic_bank_Kaupthing,_26_Sep_2008>

OFICINA DE PROGRAMAS DE INFORMACION INTERNACION DEL DEPARTAMENTO DE ESTADO DE LOS ESTADOS UNIDOS, *"La libertad de expresión en Estados Unidos"*. [en línea] <http://iipdigital.usembassy.gov/st/spanish/pamphlet/2013/04/20130419146174.html#axzz2gjCpr5p0>

AMERICAN CIVIL LIBERTIES UNION, *"Libertad de expresión",* [en línea] <https://www.aclu.org/libertad-de-expresion>