UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Doctorado en Ciencias Políticas y Sociales

LA CRIPTOGRAFÍA COMPUTACIONAL EN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN; APORTACIONES DE ALAN M. TURING Y CLAUDE E. SHANNON A SU DESARROLLO. UNA RECCONSTRUCCIÓN DESDE LA HERMENÉUTICA PROFUNDA

Tesis de doctorado

QUE PARA OPTAR POR EL GRADO DE DOCTORA

EN CIENCIAS POLÍTICAS Y SOCIALES

PRESENTA

GLORIA VALEK VALDÉS

Directora: Dra. Atocha Aliseda Llera, IIF, UNAM

Comité Tutor: Dra. Silvia Molina y Vedia, FCPyS, UNAM

Dra. Florence Toussaint Alcaraz, FCPyS, UNAM

Lectoras: Dra. Alma Rosa Alva de la Selva, FCPyS, UNAM

Dra. Graciela Martínez Matías, FCPyS, UNAM

Ciudad Universitaria, Cd. Mx., Abril de 2019

A mis tres grandes amores:

Felipe

Juan Felipe

Milena

ÍNDICE

PREFACIO

Desde 2012, cuando conocí propiamente la trayectoria de Alan Mathison Turing, hasta la fecha, me han ocurrido infinidad de cosas nuevas, interesantes, apasionantes. No sólo me introduje a fondo en la vida de uno de los científicos más reconocidos del siglo XX sino que también exploré a profundidad la obra de Claude Elwood Shannon, otro de los científicos más reconocidos por su genialidad más allá de establecer la Teoría matemática de la información. A partir de ese año, no sólo tuve la oportunidad de escribir y publicar sendos artículos sobre ambos sino que, con uno de ellos (durante el centenario de Turing), obtuve un reconocimiento en el Premio Nacional de Periodismo de Ciencia 2013.

Esta aventura, que surgió primero por la curiosidad y luego por el afán de entender a fondo a un personaje como Turing, se tornó en un proyecto de investigación de doctorado en el que incorporé a Shannon y fui entrelazando las vidas de ambos reconociendo la importancia de sus obras para las distintas áreas de estudio y en particular, para las ciencias sociales y específicamente las ciencias de la comunicación que poco, muy poco, los han reconocido.

Descubrí en el trayecto apasionantes áreas de estudio de Turing y de Shannon como la comunicación secreta y la criptografía computacional y su importancia en la historia de las tecnologías de la información y la comunicación así como su enrome trascendencia en el funcionamiento del mundo actual. En el proceso también descubrí que pese a ser grandes innovadores y dos de las personas más creativas que ha dado la humanidad en muchas áreas de la cultura se les ignora. En particular, en las ciencias de la comunicación, descubrí la omisión total de uno de mis personajes y la interpretación a medias de otro. De eso trata este trabajo de tesis porque finalmente mi propósito fue primero comprenderlos, ubicarlos en sus contextos y circunstancias y luego encontrar los fundamentos teóricos para

incorporarlos con toda su fuerza e importancia a las ciencias de la comunicación, a las ciencias sociales. Espero haberlo logrado.

En el trayecto de esta investigación conté con el apoyo de varias instituciones y personas, sin las cuales esto no hubiera sido posible. En primer lugar, mi agradecimiento infinito a la UNAM, mi querida *alma mater* y a la entrañable Universidad de Cambridge que, además de otorgarme el título de maestría en filosofía (historia) hace más de 25 años, recientemente me permitió revivir momentos mágicos cuando realicé una corta pero fructífera práctica de campo en sus instalaciones a la par que viajé a Bletchley Park y a la Universidad de Manchester para enriquecer el análisis sobre Turing; el Reino Unido siempre tendrá un significado especial en mi vida personal, académica y profesional.

También de la UNAM agradezco a la Dirección General de Divulgación de la Ciencia, mi lugar de trabajo durante más de veinte años, que me permitió cumplir el sueño, durante los últimos cuatro, de hacer el doctorado mientras trabajaba en la revista *¿Cómo ves?;* a la FCPyS, por ser mi inicio y fin y al Programa de Apoyo a Estudiantes de Posgrado (PAEP-UNAM) por permitirme vivir una experiencia que resultó no sólo interesante y enriquecedora sino también fascinante.

A mi Comité tutor gracias por apoyar y nutrir enormemente este proyecto. Sus recomendaciones fueron siempre oportunas y certeras. A Atocha Alisada Llera, por la reveladora y puntual guía; siempre compartiste mi entusiasmo y me hiciste trabajar con orden y congruencia en un área que con frecuencia me era ajena. A Silvia Molina y Vedia por las ricas charlas y atinadas observaciones académicas; a Florence Toussaint Alcaraz, por recordarme en tus seminarios la importancia de la comunicación en cualquier proyecto multidisciplinario, lo que me permitió enriquecer éste. A Alma Rosa Alva de la Selva por tus profundas y atinadas observaciones metodológicas a partir del examen de candidatura y a Graciela Martínez Matías por tu apoyo desde el inicio, tus clases y tu generosidad. Todas,

mujeres destacadas que me hicieron sentir en casa con el rigor académico que necesitaba. De todas aprendí mucho. ¡Gracias a cada una de ustedes!

A Gloria María Valdés Alcántara por tu ejemplo. A Felipe López Veneroni mi amor, admiración y agradecimiento por estar siempre; valoro enormemente tenerte en lo personal, en nuestra familia y en la parte académica, al escuchar mis inquietudes y compartir mis emociones. A Juan Felipe y a Milena gracias por existir y hacerme sentir la mamá más orgullosa y afortunada del mundo; a ustedes debo también el continuo impulso para seguir adelante.

INTRODUCCIÓN

En esta investigación indagamos, exponemos y vinculamos las aportaciones del matemático británico Alan M. Turing y del ingeniero estadounidense Claude E. Shannon a lo que denominamos *comunicación secreta*, con herramientas de la criptografía computacional y las tecnologías de la información y la comunicación (TIC) y exponemos su relevancia en las ciencias de la comunicación a partir del método hermenéutico. También y como consecuencia de ello ponemos en relieve la omisión de la que han sido objeto ambos científicos y sus descubrimientos en los programas académicos y de investigación dentro del campo de estudio de la comunicación. Para lograrlo, partimos de que la *comunicación secreta* es un fenómeno comunicativo, resultado y objeto de la criptografía computacional, que implica una *acción comunicativa* en la que los actores (emisor-receptor) buscan entenderse a partir de una clave que sólo ellos conocen.

En ese sentido, trabajamos tres ejes temáticos fundamentales que proporcionan el marco conceptual para abordar nuestra investigación como fenómeno de comunicación:

- I Contexto histórico y científico en el que se desenvolvieron Turing y Shannon. Primeros sesenta años del siglo XX (guerras mundiales, específicamente la Segunda).
- II Vida y obra de ambos científicos con énfasis en sus aportaciones a la criptografía moderna o computacional, la comunicación secreta y la información.
- III Papel de Turing y Shannon en los orígenes y desarrollo de las TIC, particularmente con respecto a la computación.

Partimos de a) la **historia** como representación discursiva que afecta nuestra interacción comunicativa y permite desentrañar los aspectos y circunstancias que llevaron a Turing a caracterizar la **noción de computabilidad** y con ello el modelo

teórico de lo que hoy son las computadoras y a Shannon la Teoría matemática de la información; b) del **revisionismo histórico**, como el estudio y reinterpretación de la historia a la luz de nuevos datos y el cambio de los valores desde los que se observa el pasado, y c) de la **hermenéutica** que estudia el mundo de las ideas, entendidas éstas como representaciones sociales de la experiencia práctica del mundo que cumplen con los siguientes aspectos:

- a) históricamente situadas (no universales);
- b) ligadas a una cosmovisión u horizonte de interpretación (pensamiento científico-analítico), y
- c) sujetas en su validación a cómo son aceptadas o rechazadas por los actores sociales y las consecuencias de estas ideas en su momento y posteriormente.

Planteamiento. La contextualización histórica de una disciplina es indispensable para comprender su estructura, su evolución y sus giros, sin los que difícilmente podríamos tener una idea clara y objetiva de sus alcances. Turing y Shannon son personajes altamente reconocidos desde campos conceptuales de las matemáticas, la ingeniería y específicamente desde las ciencias de la computación pero no desde las ciencias sociales y el estudio de las nuevas tecnologías de la información, las plataformas digitales en redes electrónicas, de la comunicación en general y particularmente de un campo poco estudiado de ella, la **comunicación secreta**, aunque la parte esencial de sus trabajos se desarrollara justamente a la par del surgimiento de la cibernética y la teoría general de sistemas –Norbert Wiener (1948), Arturo Rosenblueth (Valek, 2010)–. También sus trabajos son producto de una coyuntura histórica y un contexto social: la Inglaterra y los Estados Unidos de las primeras décadas del siglo XX y sobre todo el momento coyuntural de la Segunda Guerra Mundial.

Es pertinente pues que los ubiquemos en su justa dimensión desde las ciencias de la comunicación y que dicha ubicación ocurra a través de la divulgación de sus

aportaciones a partir de las tres categorías básicas de este análisis: el **tiempo**, el **espacio** y el **momento coyuntural** de la Segunda Guerra Mundial.

Como se ha dicho anteriormente, esta investigación busca revaluar desde la hermenéutica la importancia de las obras de Turing y Shannon respecto de la evolución de uno de los campos problemáticos más innovadores de las ciencias de la comunicación contemporánea (las **TIC**) y, al hacerlo, trazamos los nexos que las unen al problema de la codificación del lenguaje, a través de cuatro ejes conceptuales fundamentales:

1. La criptografía computacional
2. La información
3. La comunicación secreta
4. Las tecnologías de la información y comunicación

Al desentrañar los orígenes y el conjunto de condiciones históricas, intelectuales y científicas que permitieron y al mismo tiempo impulsaron a Turing y a Shannon a establecer las bases y condiciones de desarrollo de las tecnologías de la información y la comunicación que hoy forman parte central del objeto de estudio de las ciencias de la comunicación, pretendemos revalorar en su justa dimensión su importancia en nuestra área de estudio. Para ello, primero hacemos un recorrido fenomenológico por la vida y contexto sociopolítico en el que se desenvolvieron; segundo, conformamos y analizamos el corpus teórico sobre y alrededor de las TIC y tercero, logramos una construcción teórica que permite ubicar a Turing y a Shannon en las TIC, tanto en sus raíces y aspectos teóricos como en sus aplicaciones prácticas, hoy fundamentales para las ciencias de la comunicación. Finalmente, y esa es la aportación principal de esta investigación, ubicamos a la comunicación secreta y a la criptografía como importantes campos problemáticos inherentes a las ciencias de la comunicación que han sido omitidos en sus programas y áreas de estudio.

Así, esta investigación pretende ser una *reconstrucción crítico interpretativa de las condiciones históricas* (contexto) que permitieron al matemático británico y al ingeniero estadounidense plantear las bases para el desarrollo de la criptografía computacional, la comunicación secreta y las TIC en el marco de la primera mitad del siglo XX y su trascendencia en el marco general de la comunicación social.

Esto porque estamos convencidos de que comprender las tecnologías que operan como soporte material del discurso y que permiten su pluralización y extensión social, supone analizar a quienes bajo circunstancias históricas, políticas y culturales específicas, concibieron, diseñaron y sentaron las bases para el surgimiento y desarrollo de esas tecnologías.

Por otra parte, reiteramos, el periodo en el que Turing y Shannon trabajan ocurre en un momento histórico singular: el momento coyuntural de la Segunda Guerra Mundial, en el que literalmente se puso en juego la supervivencia de la cultura occidental y con ésta muchos de sus valores fundamentales (entre ellos, el del conocimiento científico, la libertad de expresión y el derecho a la información). Por todo ello, nos parece pertinente estudiarlos, contextualizarlos, entenderlos, interpretarlos y reinterpretarlos y que mejor forma de hacerlo que a partir de la hermenéutica que, de acuerdo con sus principales exponentes, en esa reflexión metodológica, el fenómeno a interpretar debe comprenderse en su contexto y a partir de la obra y biografía de los involucrados.

Partimos del supuesto de que los procesos sociales contemporáneos de comunicación, que alternan la mediación dialógica con la mediación tecnológica, están profundamente ligados a las obras de Alan Turing y Claude Shannon, quienes desarrollaron tanto la lógica base para la teoría de la computación como los principios operativos fundamentales de lo que hoy denominamos tecnologías de la información y la comunicación.

A lo largo de este trabajo de investigación vemos cómo Alan Turing proporciona

los fundamentos matemáticos, los modelos y los ***algoritmos***[1] que apuntan al uso de mecanismos digitales para cifrar y descifrar códigos y mensajes y almacenar y transmitir información mediante principios análogos a la comunicación humana. También vemos cómo Claude Shannon sienta lo que desde la corriente funcionalista se consideran las bases de la teoría convencional de la información, generando un modelo matemático que permite formalizar aspectos mecánicos de la transmisión/recepción de señales en determinados entornos electromagnéticos.

Así, al construir el contexto general del tema y ubicar a los autores, conceptos, nociones y textos sobre los distintos subtemas, el **objetivo general** de esta investigación se acotó de la siguiente manera:

Analizar y contextualizar, desde la perspectiva de una historia de las tecnologías de la información y la comunicación, las aportaciones fundamentales de dos de los científicos más influyentes del siglo XX, para la creación, consolidación y desarrollo de una nueva cultura en la que el lenguaje, la tecnología y la sociedad convergen para dar forma al perfil de la llamada *sociedad de la información*[2] y las TIC. En este sentido, la presente investigación no busca profundizar en el desarrollo o los usos sociales de las TIC, sino en sus orígenes y, particularmente, en el conjunto de condiciones históricas, intelectuales y científicas que permitieron y, al mismo tiempo, impulsaron a Alan M. Turing y a Claude E. Shannon a establecer las bases y condiciones de posibilidad de las tecnologías que hoy forman parte central del objeto de estudio de las ciencias de la comunicación. En esta investigación también pretendemos ampliar el campo de estudio de las ciencias de la comunicación al incluir en sus temáticas tanto a la criptografía computacional como a la comunicación secreta.

De esa manera, partimos de la siguiente premisa: **como iremos argumentando a**

[1] Todos los términos o conceptos en cursivas se explican al final de esta investigación, en su correspondiente Glosario.
[2] Sobre la Sociedad de la información ahondamos más adelante.

lo largo de este trabajo de investigación, mediante sus investigaciones secretas y su afán por romper esquemas y traspasar límites, Alan M. Turing se adelantó a su tiempo al desarrollar teorías, instrumentos y máquinas de decodificación del lenguaje, que darían pie a las bases de las TIC, sin las cuales hoy no se podría entender el mundo. Las TIC de hoy no serían posibles sin el trabajo teórico desarrollado por Turing en las primeras décadas del siglo XX que darían pie a las computadoras. Por tanto, este científico, al que se ignora en los estudios de comunicación, debería ser uno de los pilares de nuestro bagaje teórico. Dichas tecnologías tampoco podrían haberse desarrollado sin los trabajos criptográficos y la Teoría matemática de la información expresada por Shannon.

Si bien, a lo largo de este trabajo, mencionamos las aportaciones tanto de Turing como de Shannon en distintas áreas de la ciencia, centramos nuestros puntos de análisis en los ejes de esta investigación: la criptografía computacional y la comunicación secreta, aspectos que, reiteramos, deben formar parte obligada del campo de estudio de las ciencias de la comunicación.

Análisis hermenéutico. A lo largo de este trabajo vamos incorporando conceptos y categorías pertinentes para hacer visible el nexo que existe entre las aportaciones de Turing y las de Shannon a las TIC y a la comunicación secreta. El análisis hermenéutico del impacto de las aportaciones criptográficas de Turing y de Shannon a las TIC, específicamente en cuanto al desarrollo de los ***códigos binarios*** y la computadora, se realiza con base en las nociones de ***programa*** y ***algoritmo***.

En el primer capítulo partimos, con el filósofo alemán Wilhelm Dilthey (1833-1911), de una "conciencia histórica" de "re-vivir desde nuestro propio sitio y circunstancia una historia de vida ajena o distante" (Lince y Amador, 2013ª, 13 y Dilthey,

Wilhelm, 2010) y con J. B. Thompson[3] de que el modelo de análisis hermenéutico (interpretativo).

Se retoma la corriente idealista subjetiva y al filósofo Edmund Gustav Husserl (1859-1938), quien siguió a los neo-kantianos alemanes de fines del siglo XIX. Además de este último y del propio Dilthey, hay otros autores que han desarrollado este método comprensivo, como Weber, Gadamer y Paul Ricoeur quien, en su *Teoría de la interpretación,* desarrolló el modelo que posteriormente John B. Thompson explica desde tres ángulos que resultan muy pertinentes para nuestro análisis: el contexto sociohistórico; el análisis formal discursivo y la interpretación y reinterpretación.

Con respecto a la teoría filosófica de la hermenéutica, ubicamos como antecedentes algunas de las definiciones del *Diccionario Interdisciplinar de Hermenéutica* (dirigido por A. Ortiz-Osés y P. Lanceros, en 2006), donde se toman en cuenta categorías planteadas por autores como Heidegger (fundador de la hermenéutica contemporánea), Gadamer, Ricoeur, Durand y otros hermeneutas para proporcionar una introducción a esa teoría filosófica.

También ha sido de gran apoyo La *Historia de la hermenéutica* de Maurizio Ferraris (1999 y 2002) y reflexiones sobre sus exponentes y principales ideas. De H.G. Gadamer consultamos *Verdad y método* (1966); de Paul Ricœur "La explicación y la comprensión" (1995) y de John B. Thompson, sus textos sobre hermenéutica, en especial los dedicados a la metodología de la interpretación y la hermenéutica profunda (2003. 2010).

Desde las teorías del revisionismo histórico hicimos una reconstrucción histórica de la influencia de Turing y de Shannon en las teorías sistémico funcionalistas de la comunicación. Tomamos a la cibernética y a la teoría de sistemas sólo como

[3] Véase su Capítulo VI "La metodología de la interpretación"*, en Ideología y cultura moderna* (2002).

puntos de partida para luego abordar los nexos con las aportaciones de Turing y Shannon en el marco de la Segunda Guerra Mundial.

Hermenéutica profunda. Como explicamos anteriormente, nuestro punto de aterrizaje metodológico se centra en "La metodología de la interpretación" de John B. Thompson donde, con base en el trabajo de otros hermeneutas demuestra que la *hermenéutica profunda* permite un marco en el cual se pueden interrelacionar diferentes métodos de análisis y sus ventajas y límites proporcionando un marco metodológico general.

- Para mostrar el papel relevante de la hermenéutica en la investigación sociohistórica, con Thompson retomamos a Dilthey, Heidegger, Gadamer y Ricoeur.
- Con la hermenéutica partimos de que muchos fenómenos son formas simbólicas que suscitan problemas de comprensión e interpretación y que en particular en las ciencias sociales el objeto de nuestras investigaciones es en sí mismo un campo preinterpretado (Thompson, 2012).
- Tomamos en cuenta los tres aportes de Husserl a la hermenéutica: 1) El sentido y significado de un hecho, de una palabra están predeterminados por su horizonte de donación; 2) Lo presupuesto como *suelo* de toda experiencia y horizonte de todo *darse* con sentido, es el mundo de la vida cotidiana (*Lebenswelt*), y 3) todo comprender presupone una *precomprensión* del mundo, articulada de antemano lingüísticamente.

Retomamos de manera general y sólo como referencia los textos de Umberto Eco *Interpretación y sobreinterpretación* (1995) y sus reflexiones sobre interpretación e historia. Cabe aclarar que si bien no realizamos un análisis semiótico, con Eco (2000) partimos de que la semiótica estudia los procesos culturales como procesos de comunicación. El mismo autor explica que bajo los procesos culturales hay sistemas y que la dialéctica entre sistemas y procesos nos lleva a afirmar la dialéctica entre códigos y mensajes. Retomamos lo que Eco llama

lenguajes formalizados que parten del estudio de las estructuras matemáticas[4] para llegar a los lenguajes artificiales (con un valor convencional para poder transmitirse).

Tomamos en cuenta la emisión de mensajes basados en códigos, que modifican la semántica de un lenguaje ya dado o generan una nueva semántica mediante la recodificación y pueden ser considerados subyacentes o metalenguajes (generados, artificiales, no naturales como el código Morse).

En el momento en que fue necesario para los fines de esta investigación, con Eco (2001) y Miller[5] tomamos al código como un sistema de símbolos que por convención previa está destinado a representar, a transmitir la información desde la fuente al punto de destino.

Aportaciones de Turing y Shannon a las TIC. Alan Mathison Turing (1912-1954) es uno de los científicos más reconocidos por distintas áreas de la ciencia. Como veremos más adelante, además de ser un destacado matemático y lógico, sin sus trabajos de investigación, desarrollados en la primera mitad del siglo XX, las actuales tecnologías o plataformas sobre las que operan Internet, las redes sociales (*blogs, facebook, twitter, my space*, etc.) y en general todo lo relativo a sistemas de cómputo electrónico, no hubieran tenido un desarrollo tan acelerado y un despliegue tan amplio.

Por su parte, a Claude Elwood Shannon (1916-2001) se le reconoce ampliamente desde la ingeniería y la computación pero tampoco han sido valoradas a cabalidad sus aportaciones a las ciencias de la comunicación pues su famosa Teoría de la información, a la que dedicamos varios apartados más adelante, creó falsas expectativas y se le exigió en su momento abarcar campos sociológicos que escapaban de su interés y áreas de estudio.

[4] Que Eco (2000) retoma de otros autores como Prieto (1966), Gross Lentin (1967) y Bertin (1967).
[5] Citado por el mismo Eco (2000).

A partir de la investigación bibliográfica y documental, en las páginas siguientes analizamos, interpretamos y reinterpretamos las vidas y obras de ambos personajes, específicamente con respecto a sus aportes a la criptografía computacional y a las TIC. En cuanto al matemático británico nos adentramos en su concepción de la llamada *prueba de Turing* y en el diseño y desarrollo de la *Bomba*, máquina eletromecánica con la que le fue posible determinar la posición inicial de los rotores y funcionamiento de la máquina alemana Enigma.

Además de varios textos especializados, retomamos a los principales biógrafos de Turing. El primero, y quizás el de mayor relevancia, es Andrew Hodges, quien lo rescata del olvido con *Alan Turing: The Enigma* (1983, 2012). Seguimos con D. Leavitt, con *The man who knew too much: Alan Turing and the invention of the computer* (2006), *y* en castellano, con Rafael Lahoz-Beltrá, autor de *Turing. Del primer ordenador a la inteligencia artificial* (2005), que plantea la participación del matemático inglés en el desarrollo de Colossus que, según las últimas revisiones históricas, ha pasado a ser considerada como la primera computadora programable de la historia, incluso anterior a ENIAC y a otras máquinas estadounidenses. (Lavington, 2016)

Sobre Turing encontramos innumerables textos especializados en las áreas de matemáticas y computación pero escasos documentos académicos o de divulgación en ciencias sociales. De las fuentes originales sobre las ideas y textos escritos por el propio Turing y relacionados indirectamente con las TIC, nos basamos en:

- 1. Turing, A.M., “Intelligent Machinery”, en Ince D.C. (editor, 1992), *Collected Works of A.M*. Turing-Mechanical Intelligence.
- 2. Turing. A. (1950), “Computing machinery and intelligence”, *Mind*, 59:433-460.
- 3. Testamento de Turing.

- 4. www.itpro.co.uk/631417/turing-papers-saved-for-bletchley, (escritos d e Turing s ecretos durante varias déc adas), d el National Heritage Memorial Fund y que permanecen en Bletchley Park.
- 5. Wikipedia, Turing Machine: htto://en.wikipedia.org/wiki/Turing_machine[6]

Después de haberlo ubicado en su contexto (espacial y temporal), en las TIC y la criptografía c omputacional (Capítulos I al I II), en el c apítulo I V analizamos c on detenimiento el ar tículo de T uring, publ icado en 19 50 en l a r evista de filosofía *Mind,* titulado " Maquinaria c omputacional e i nteligencia", q ue p ropone s ituar l a pregunta sobre la inteligencia mecánica en una versión del *juego de imitación*, lo que se conoce ahora como *Prueba de Turing*. Con la académica y estudiosa de la lógica m atemática, A tocha A liseda, p artimos de lo q ue el la a s u ve z retoma d e otros a utores s obre el hec ho de que es a *prueba* se c onsidera un pi lar pa ra plantear l a analogía "la mente es como una computadora", que sirvió de pu ente entre l a filosofía d e l a m ente y l a inteligencia ar tificial. La pr imera pr oporcionó l a base c onceptual; l a s egunda, l as her ramientas para r epresentar y m anipular e l conocimiento (Aliseda Llera, 2007 y 2013, 10-17).

Por ot ra par te, d el l ado oeste del A tlántico, en 19 48, c on s u artículo " Teoría matemática d e l a c omunicación", C laude E lwood S hannon d emostró q ue l a información podía definirse y medirse desde el punto de vista científico por medio de ***dígitos binarios***. Así nació la Teoría de la información, que hoy tiene diversas aplicaciones en t odas las áreas del conocimiento y en nues tra vida cotidiana. Su interés s e c entró en as pectos t écnicos, pero t ambién hi zo c ontribuciones a

[6] De los textos y documentos de Turing, uno de los más importantes desde el punto de vista matemático es "On Computable Numbers, with an Application to the Enstscheidungsproblem" (indecibilidad), escrito entre 1936 y 1937. Sin embargo, pese a su trascendencia, no lo consideramos aquí debido a su alta especialización y porque escapa a los objetivos de este trabajo.

campos como la criptografía, la computación y la inteligencia artificial[7], de la que fue partícipe en sus inicios[8]: a las TIC.

El análisis específico de la vida y obra de Shannon se basa también en sus principales biógrafos y textos, particularmente en su *Teoría de la criptografía* y la *Teoría matemática de la comunicación*, concebidas entre 1948 y 1949. Esta última fue editada en 1949, cuando el sociólogo Warren Weber escribió la introducción de la famosa teoría y se hizo coautor. La obra criptográfica que Shannon había escrito durante y después de la guerra se desclasificó años después.[9]

Sobre las TIC. Ubicar la historia y desarrollo de las TIC ayudó a enmarcar el contexto sociohistórico de la comunicación secreta, la criptografía computacional y las aportaciones de nuestros personajes. Sobre las TIC encontramos una extensa bibliografía desde la computación, las matemáticas y la historia general de la comunicación como puntos de partida para encontrar el nexo entre el trabajo tanto de Turing como de Shannon. Para ello nos basamos en el bagaje teórico y los conceptos de F.C. Williams (1975) que pone énfasis en la importancia de Colossus y ACE en el desarrollo de las primeras computadoras; Briggs, A. y P. Burke (2002) *De Gutenberg a Internet*, que contiene una historia social de los medios de comunicación; Bustamante, E. (2002), *Comunicación y cultura en la era digital,* y de Castells, M. (1999), "Internet y la sociedad red"; como lección inaugural del programa de doctorado sobre la sociedad de la información y el

[7] Véase el artículo "Emerge una nueva disciplina: las ciencias cognitivas", de Atocha Aliseda (2007) publicado en la revista *Ciencias* de la UNAM.

[8] De la participación de Shannon en la inteligencia artificial se sabe poco pero incluso tuvo que ver con el nombre de esta nueva disciplina y sus primeros avances. Véase, entre otros, Guillén Torres, Beatriz, (2016) "El verdadero padre de la Inteligencia Artificial", en Ventana del conocimiento, donde explica que "El texto inaugural (de esta disciplina) lo realiza junto a Marvin Minsky y Claude Shannon**,** dos prestigiosos científicos que pronto abandonaron el estudio de este campo para orientarse hacia la computación o la teorización matemática. Sin embargo, McCarthy se consagra como padre de la inteligencia artificial no solo por lograr abrir y convertirlo en un campo de investigación nuevo, sino por seguir aportando evidencias para su desarrollo durante medio siglo"

[9] Warren Weaver (1894-1978) tuvo gran importancia para la culminación y el asentamiento de la Teoría Matemática de la Comunicación de 1949, hoy conocida por todos como la Teoría de la Información. Weaver enriqueció el planteamiento inicial de Shannon, que se restringía al ámbito de los lenguajes máquina, y la consecuente transmisión de estos mensajes. A estos dos autores se les debe el esquema lineal de la comunicación: *Fuente/codificador/mensaje-canal/descodificador/destino*.

conocimiento; De Moragas, M. (1997) "Las ciencias de la comunicación en la sociedad de la información", y de Dix, A. *et al* (2004) *Human-computer interaction.* De R. T. Griffiths, (2002) *History of Internet, Internet for historians* y del teórico de la comunicación Armand Mattelart (2001), *Historia de la sociedad de la información*, de donde se retoman algunos conceptos básicos. De Alva de la Selva, A.R. (2015): *Telecomunicaciones y TIC en México*.

El capítulo III se centra en los principales modelos y escuelas de las ciencias de la comunicación con respecto a la omisión de Turing y a la interpretación errónea de Shannon en ellos. Seguimos en el capítulo IV con la descripción de las TIC y posteriormente con la criptografía computacional y la comunicación secreta.

Para ubicar la historia y el desarrollo de la criptografía nos basamos en autores como Martin Reina (2003 y 2009) y en David Kahn (1967 y 1996) en cuanto a definiciones sobre ***cifra, código*** y ***mensajes secretos*** y su exhaustivo análisis de la historia de la criptografía, desde el antiguo Egipto a los años 60 del siglo XX y la batalla de los criptoanalistas Aliados contra las potencias del Eje durante la Segunda Guerra Mundial. De Daniel Martín Reina (2009), David Newton, B.J. Copeland y Simon Singh retomamos sus recorridos conceptuales e históricos por la criptografía y la ciencia de los mensajes secretos. También de Marian Rejewski (1981) y Robert Harris, el papel de los polacos y Enigma. La batalla desde Bletchley Park con los códigos secretos del ejército y marina alemanes fue apasionante y tratamos de narrarla la manera más objetivamente posible.[10]

Como hemos acotado, otro eje central de esta investigación se refiere a la comunicación secreta como fenómeno comunicativo, resultado y objeto de la criptografía computacional. En su apartado correspondiente, ubicamos las aportaciones del matemático británico y del ingeniero estadounidense en lo referente a la *comunicación secreta*, entendida ésta como un fenómeno

[10] Cabe mencionar aquí que tuvimos la oportunidad de visitar esas enigmáticas instalaciones durante una práctica de campo en mayo-junio de 2018, lo que nos dejó experiencias sumamente enriquecedoras que vamos plasmando a lo largo de este trabajo de investigación.

comunicativo producto de una práctica social. (Gallego Dueñas, 2012). Para lograrlo, partimos del secreto como una forma de relacionarnos los seres humanos "…en la que un actor o actores, en una determinada situación, evitan, limitan o modifican la comunicación de algo (acción, pensamiento, sentimiento…) a otro actor o actores, durante cierto tiempo, haciendo uso de ciertas tácticas, es decir, suponiendo un esfuerzo. Y no sólo cuando lo compartimos sino en todo momento, guardándolo, compartiéndolo y desvelándolo." (Gallego Dueñas, 2012, 3).

Tomamos en cuenta algunos aspectos lingüísticos y al académico Beryl L. Bellman (1981, 1-24), al definir la importancia del lenguaje en el secreto pues mantiene que esa secrecía debe ser vista como un método para manejar información oculta en un contexto determinado, con un contexto de significado. Así, un secreto, para serlo, debe tratar sobre una información relevante. Pero, como explica Gallego Dueñas, no es una cualidad de la información sino del modo en que esa información se transmite. "Por eso hablamos de *plusvalía simbólica*[11] cuando hablamos de secreto, y a que no sólo se trata de ocultar cosas que consideramos valiosas, sino que, sobre todo, se otorga un valor extra a aquellas cosas que se convierten en secreto".[12]

Dado que la criptografía consiste precisamente en la transmisión de un lenguaje secreto y que su método es el cifrado, analizamos cómo éste enmascara las referencias originales de la lengua por un método de conversión de un algoritmo que permita el proceso inverso o cifrado y cuyo uso posibilita el intercambio de mensajes que sólo pueden ser entendidos por los destinatarios que poseen la clave. Esta última basada en un ***libro de códigos***. Específicamente en el tema de nuestro interés, es decir, la criptografía en los lenguajes secretos, seguimos de la mano de Gallego Dueñas, que pone de manifiesto que a través de la criptografía no sólo se oculta el mensaje, sino también se oculta la cifra, la clave de su

[11] El Diccionario de la Real Academia Española (RAE) se refiere a la plusvalía como el aumento del valor de un objeto o cosa por motivos extrínsecos a ellos. Más adelante, explicaremos su acepción simbólica.
[12] "Hay oferta de información a unos receptores que la demandan –o mejor, a los que incita a demandar…" (Gallego Dueñas 2012, 13).

entendimiento y que una de las técnicas más importantes conceptualmente es el *secret sharing.* (Gómez, 2010 y Cascudo, 2010). Como lo vemos más adelante, ese método consiste en la distribución de un mensaje entre un grupo de participantes, cada uno de los cuales tiene una parte. El mensaje sólo puede reconstruirse cuando se combinan un número suficiente de partes pues solas carecen de utilidad. “Desde el punto de vista formal, en el esquema del *secret sharing* hay un emisor (*delaer*) y n actores (*players*). El emisor entrega el secreto a los actores, pero sólo cuando se cumplan una serie específica de condiciones”. (Gallego Dueñas 2012, 10).

Así, en esta investigación tratamos al secreto no sólo como una forma de comunicar, sino como una manera que despierta el deseo de conocimiento, que genera una *plusvalía simbólica* y que debemos integrar formalmente hoy más que nunca a los estudios de comunicación, reconociendo cabalmente las aportaciones de Turing y Shannon a su desarrollo.

Capítulo I

La teoría de la interpretación como estrategia metodológica de análisis

[…] una historia debe ser más que una enumeración de acontecimientos en serie; ella debe organizarlos en una totalidad inteligible, de modo que se pueda conocer en cada momento el "tema" de la historia. En resumen: la construcción de la trama es la operación que extrae de la simple sucesión la configuración (Paul Ricœur, 1995).

En este primer capítulo se describe la estrategia metodológica que se siguió en esta investigación para establecer la ignorada conexión de las tecnologías de la información y la comunicación (TIC), la criptografía computacional y la comunicación secreta con las aportaciones del matemático británico Alan M. Turing y el ingeniero estadounidense Claude E. Shannon para su desarrollo. Como se explica en este apartado, esto se hace desde el marco metodológico de la hermenéutica profunda particularmente desde los planteamientos del sociólogo anglosajón John B. Thompson y los conceptos de otros hermeneutas como H. G. Gadamer y Paul Ricoeur.[13]

En este capítulo pretendemos empezar a responder las siguientes preguntas: **¿Qué relación guarda hoy en día el trabajo teórico y práctico desarrollado en las décadas de 1940-50 por científicos como Alan Turing y Claude Shannon en materia de la transmisión, ordenamiento, codificación y decodificación de grandes cantidades de información mediante sistemas electrónicos automáticos? ¿Puede hoy, a la luz del uso social cada vez más extendido de las TIC revalorarse el modelo de la teoría matemática de la información y las**

[13] Entre otros, de Thompson (2002): "La metodología de la interpretación",; de Gadamer (1987): *Verdad y método,* y de Paul Ricoeur (1966) *Tiempo y narración*.

contribuciones al desarrollo de las computadoras, elaborados por Turing y por Shannon antes, durante y poco después de la Segunda Guerra Mundial?

Partimos, entonces, de la siguiente hipótesis general: **Si bien la teoría convencional de la comunicación de Harold Laswell[14], ha sido ampliamente cuestionada por diversas escuelas de pensamiento[15] (dado que explica la comunicación humana extrapolando a las relaciones sociales el modelo matemático de la información, desarrollado por Shannon y Weaver[16]), los acelerados avances en las nuevas TIC ponen en relieve la ignorada contribución en nuestro campo de estudio de la comunicación social tanto del matemático británico Alan Turing[17] como del ingeniero estadounidense Claude Shannon. El primero, a través de la criptografía y la computación, el segundo, por la validez conceptual del modelo matemático de la información permitiéndonos ambos una comprensión más sólida del proceso de la interacción social que se realiza a través de las plataformas digitales que operan en las redes electrónicas actuales.**

A este efecto, esta investigación constituye una reconstrucción histórico-hermenéutica del trabajo intelectual y práctico que se llevó a cabo en aquellos años y que hoy, más de siete décadas después, parece desplegarse no sólo en sus aplicaciones técnicas, sino en el impacto social y cultural que tienen las TIC en las interacciones sociales cotidianas, así como en los procesos administrativos, la educación y el desarrollo de la cultura.

Si bien no se trata de revalorar el paradigma de Laswell,[18] sí resulta necesario analizar cómo el modelo de la teoría matemática de la información y las

[14] https://www.businesstopia.net/communication/lasswell-communication-model.
[15] Véase de Armand Mattelart y Michelle Mattelart (1997): y https://www.businesstopia.net/communication/shannon-and-weaver-model-communication
[16] Cfr. https://www.businesstopia.net/communication/shannon-and-weaver-model-communication
[17] http://www.wired.co.uk/article/turing-contributions.
[18] Como veremos en el capítulo III de este trabajo, el modelo o paradigma que dio a conocer Harold D. Lasswell (1902-1978) en 1948 se refiere a un proceso, simplificado en cuatro preguntas: ¿quién dice qué?,

contribuciones de Alan Turing y del propio Shannon a la criptografía y a la computación tienen hoy una nueva pertinencia conceptual en relación al acelerado desarrollo y al fuerte impacto de las TIC en la interacción social.

Aquí vale la pena volver a hacer notar que en esta investigación estudiamos de qué manera el trabajo desarrollado tanto por Turing como por Shannon sentó las bases operacionales no de una teoría de la comunicación humana desde el punto de vista sociológico o antropológico, pero sí de las tecnologías que han hecho operativas, a gran escala, las plataformas digitales que, a través de las redes electrónicas, constituyen el espacio práctico en el que se llevan a cabo innumerables interacciones discursivas o comunicacionales: desde la reproducción instantánea de noticias y datos de todo tipo, hasta el intercambio y almacenamiento de información pública o confidencial, pasando por el intercambio dialógico de opiniones, argumentos y deliberaciones que afectan la práctica política y las relaciones sociales cotidianas.

Todo esto se hace en función de la pertinencia (más urgente que nunca, dado el desarrollo de las TIC) del estudio de la **comunicación secreta** (otra de nuestras categorías y que desarrollamos en el capítulo V de esta investigación) como una forma de interacción cada vez más común en nuestra vida profesional, académica y cotidiana desde su uso diario en operaciones bancarias hasta en el acceso restringido (secreto) a las redes digitales y los servicios de información. Esta reconsideración nos lleva a sustentar en los capítulos siguientes, sobre todo en los capítulos V y VI, a la comunicación secreta como un nuevo campo de estudio, imprescindible hoy en las ciencias de la comunicación.

¿por cuál canal?, ¿a quién?, ¿con qué efecto? Su modelo se desarrolla después de las dos guerras mundiales, por lo que profundiza en la construcción de la comunicación propagandística, política, interiorizándose además sobre el discurso periodístico y la construcción de los enunciados religiosos, analizando los alcances de estas comunicaciones, como discursos persuasivos con una búsqueda pre-definida de resultados perentorios y de alcance masivo. Se trata de un proceso unidireccional de la comunicación. Mensajes masivos y uniformes, de orden político, periodístico, religioso. Inteligencia desde el emisor y pasividad del receptor pues es considerado masivamente. Carece de interacción y se busca una reacción esperada, única.

Pese a su trascendencia en el origen de las TIC y por tanto de las actuales formas y medios que hacen posible que hoy nos comuniquemos, el que ni a Turing ni a Shannon se les estudie a profundidad desde las ciencias sociales como personajes esenciales para entender el proceso de comprensión del estudio de la transmisión de la información y la comunicación humana. Esto se debe a varias razones, que vamos desentrañando en las páginas siguientes pero que por lo pronto centramos en un aspecto que escapó de sus propios objetivos y propósitos: la secrecía[19] de las investigaciones durante la guerra; el fallecimiento temprano de Turing (a los 41 años de edad) y el hecho de que, sobre todo en el caso de Shannon, nunca pretendiera crear una teoría de la comunicación social y fuera juzgado injustamente desde las ciencias sociales. Por todo ello no se les da la importancia que merecen como creadores de los sustentos matemáticos y técnicos que dieron origen a los actuales medios de transmisión de información y de la comunicación.

Recordemos aquí que nuestro acercamiento metodológico parte del análisis y contextualización, desde la historia como representación discursiva que afecta la interacción comunicativa y permite desentrañar los aspectos y circunstancias que llevaron a Turing a plantear el desarrollo de las máquinas computables y a Shannon la Teoría matemática de la información. Seguimos con la ubicación espacio temporal de Turing y de Shannon, acercándonos a la relación intrínseca que tienen en un momento coyuntural con respecto al desarrollo de la criptografía computacional, la comunicación secreta y las TIC, parte esencial de la comunicación actual, aspectos en los que profundizamos en los capítulos IV y V de este trabajo.

I.1. El modelo de análisis hermenéutico y nuestras categorías generales

En esta investigación partimos de la hermenéutica que, como sabemos, estudia el mundo de las ideas, entendidas éstas como representaciones sociales de la

[19]Debido a que ambos trabajaron áreas que en su momento eran secretas y estaban ceñidas a programas específicos de sus gobiernos en tiempos de guerra, sus trabajos de investigación fueron documentos ocultos y clasificados durante varias décadas.

experiencia práctica del mundo a) **históricamente situadas** (no universales); b) ligadas a una cosmovisión u **horizonte de interpretación** (no es lo mismo, por ejemplo, el pensamiento científico-analítico que el mítico), y c) sujetas en su validación por cómo son aceptadas o rechazadas por los **actores sociales** y las consecuencias de estas ideas tanto en su momento como posteriormente. Con el teórico italiano Maurizio Ferraris partimos del hecho de que "Para la hermenéutica…el problema no es tanto ver lo que hay, sino señalar que, detrás de cuanto se nos muestra como evidente, hay algo oscuro, o al menos, escondido; hay algo que es "otro" respecto de nosotros en el tiempo o en el alma: de manera que queda excluida una comprensión inmediata…"[20]

En la reflexión metodológica que implica la hermenéutica (Grondin, J., 2008: 18), al abordar la construcción del discurso histórico y la comunicación secreta alrededor de Turing y de Shannon, partimos de la historia como representación discursiva que afecta nuestra interacción comunicativa y permite desentrañar los aspectos y circunstancias que llevaron al primero a plantear el desarrollo de las máquinas computables (computadoras) y al segundo su Teoría matemática de la información. Por ello, al utilizar el modelo de análisis hermenéutico, es decir interpretativo, siguiendo a Thompson, más que buscar relaciones causa-efecto, buscamos **reconstruir históricamente** el origen y evolución de las **formas de pensamiento**; conectar éstas con las acciones sociales relevantes y establecer una conexión de sentido fundamentada en la relación **texto-contexto** (círculo hermenéutico). Lo anterior lo hacemos para **comprender** más que explicar cómo se modifica la percepción social del mundo y su acción en éste a partir de las ideas.

Dado que la hermenéutica de la vida cotidiana es el punto de partida primordial e inevitable del enfoque de la *hermenéutica profunda*, es decir, basado en la idea de que en la investigación el proceso de interpretación exige ser mediado por una

[20] Véase la relación entre hechos e interpretaciones en Ferraris, Maurizio (1999). Como ejemplos podemos referirnos al rechazo inicial de las ideas y aportaciones de científicos de la envergadura de Galileo y Darwin en sus respectivos momentos históricos.

gama de métodos explicativos u *objetivantes*, debe tomarse en consideración la manera en que las formas simbólicas son interpretadas y comprendidas por los individuos que las producen y las reciben en el curso de sus vidas cotidianas (Thompson, 2002 y Grondin, 2008).

Pasemos entonces a *objetivar* en nuestro caso específico de estudio las fases o procedimientos principales que comprenden la hermenéutica profunda; es decir, las dimensiones analíticamente distintas del proceso interpretativo. Aunque varios teóricos han desarrollado este método comprensivo, el modelo más acorde con nuestros propósitos analíticos de investigación lo desarrolló Paul Ricoeur en su *Teoría de la interpretación* (Ricoeur, 2004) que posteriormente John B. Thompson (2002) explicó desde los tres ángulos, dos de los cuales –el primero y el último– son eje de nuestra investigación: el **contexto socio histórico**; el **análisis formal discursivo** y la **interpretación y reinterpretación**.

Partimos de que la comprensión y la interpretación no son sólo métodos que podemos encontrar en las ciencias sociales y las humanidades sino también en los procesos que significan la presencia del ser humano (Grondin, p. 19). Se retoma lo anterior como punto de partida para luego abordar, desde el punto de vista histórico, a Turing y a Shannon en el momento coyuntural de la Segunda Guerra Mundial. Dado que dos de nuestras **categorías generales de análisis** son el **tiempo y el espacio** en un momento coyuntural específico, se retoman las teorías del revisionismo histórico, como el estudio y reinterpretación de la historia a la luz de nuevos datos y el cambio de los valores desde los que se observa el pasado.

Como lo retomamos aquí, el revisionismo histórico, es el estudio crítico de los hechos históricos y los relatos oficiales, con el fin de revisarlos y eventualmente reinterpretarlos. Este acercamiento metodológico tiene un uso académico legítimo y otro peyorativo. Aquí abordamos su uso académico como la reinterpretación de hechos históricos a la luz de nuevos datos, o nuevos análisis más precisos o

menos sesgados de datos conocidos. Para ello retomamos a varios autores, incluso historiadores marxistas como Eric Hobsbawm (1994).

Debido a que una categoría (Hernández, Pablo María, 1996) es cualquier sistema de clasificación jerárquicamente ordenado según la relevancia que tengan para ese sistema los diferentes elementos que lo integran, para *ubicar* (entender, comprender) la relevancia de Turing y de Shannon, partimos también de las siguientes: **Ciencia** y epistemología (efecto que guardan las aportaciones de Turing y Shannon con la teoría del conocimiento), integrada por la lógica formal; la lógica matemática y el lenguaje artificial (la criptografía). Así volvemos a la pregunta: ¿De qué manera Turing y Shannon participan y/o modifican el pensamiento científico a partir de la posición que ocupan dentro de éste (i.e.: lógica matemática/lenguaje artificial y consecuentemente inteligencia artificial-criptografía) y cómo lo modifican? **Tecnología** (desarrollos tecnológicos *derivados del pensamiento y la investigación científica* como la computadora y lo que la hace posible: el desarrollo de un lenguaje artificial como mecanismo que permite encriptar/desencriptar la información.

De estas categorías surgen las siguientes preguntas: ¿Cuáles son las características particulares que se derivan de la teoría matemática de la información y la informática como mecanismos más avanzados para codificar y operar información respecto de tecnologías anteriores: el ábaco, el código Morse, los códigos antiguos de señales marinas? Partimos del hecho de que la computación es un desarrollo tecnológico al que se llega no por accidente sino como consecuencia del avance del pensamiento científico del Siglo XX y, en particular, de la lógica matemática y de la filosofía analítica (que estudia la estructura lógica sobre la que descansa el orden lingüístico).

También se toman en cuenta los **efectos prácticos o utilidad social de una tecnología.** Aquí se pueden hacer las siguientes precisiones: *utilidad restringida o discreta* (por ejemplo, el uso del átomo como energía, medicina, arma, que tiene

enormes efectos sociales, pero que pocos especialistas pueden desarrollar) y *utilidad abierta o generalizada* (como las computadoras y sus sistemas operativos, las plataformas digitales y las redes electrónicas a las que es relativamente sencillo acceder).[21]

Otra categoría, derivada de las anteriores, es el orden o **sistema de clasificación de las ciencias**, contra lo que se pueden medir los efectos académicos de las aportaciones de Turing y de Shannon: por ejemplo, el efecto *epistemológico* del desarrollo de la computación en las ciencias naturales (inteligencia artificial); las ciencias sociales (comunicación, lingüística); las ingenierías (sistemas); la interdisciplina (nanotecnología, microchips para fines médicos, etc.). Aquí vale la pena preguntarse si surgieron nuevas disciplinas y cómo se modificó el campo u objeto de estudio de las disciplinas ya existentes.

Todas estas categorías se van analizando a lo largo de este trabajo de investigación y en función de nuestro particular objeto de estudio. Hacemos una reconstrucción histórica desde la hermenéutica de la influencia de Turing y de Shannon en las teorías sistémico funcionalistas[22] de la comunicación que vamos ubicando más adelante como soportes de nuevas formas discursivas. Recordemos que esta investigación es una reconstrucción crítico interpretativa de las condiciones históricas (contexto) que permitieron al matemático británico y al ingeniero estadounidense plantear las bases para el desarrollo de las TIC en el contexto de los primeros sesenta años del siglo XX. Que pretendemos, en pocas palabras, revalorar la importancia de las aportaciones de ambos científicos en las ciencias sociales y específicamente en las ciencias de la comunicación, como fenómenos comunicativos fundamentales para nuestra área de estudio.

[21] La mejor prueba de ello es que, una vez desarrollada la computadora y dominado el código fundamental de su lenguaje artificial (código binario: 1/0), no fueron grandes científicos teóricos, pero sí personas con una formación técnica de alto nivel, los que dieron el siguiente paso al popularizar la computación mediante equipos (Jobs) y programas (Gates) personales de fácil acceso.

[22] Véase, entre otros Karam, Tanius y sus recuadros sobre los principales teóricos de la comunicación en "Una introducción al estudio de la epistemología de la comunicación desde la obra de Manuel Martín Serrano", 253-264.

Al acotar nuestro objeto de investigación, con el filósofo alemán F. Schleiermacher (1768-1834) partimos de que nuestra interpretación debe tener límites y basarse en un contexto; en nuestro caso, a partir de la biografía y obra de los sujetos a interpretar pues "…es necesario comprender el espíritu de una época si se quiere interpretar una obra" (Grondin, 2008, p. 36). Y para ello, apelamos a una *conciencia histórica,* a la capacidad de comprender, que significa con Dilthey "re-vivir desde nuestro propio sitio y circunstancia una historia de vida ajena o distante" (Lince Campillo, Rosa Ma. y Julio Amador Bech, 2012: p.13).

En este sentido, para comprender la esencia de las **TIC** (otra de nuestras categorías generales y que desarrollamos en el capítulo IV), las tomamos como operadoras y soportes del discurso social, que permiten su pluralización y extensión; analizamos a nuestros objetos de estudio como personajes que, bajo circunstancias históricas, políticas y culturales específicas, concibieron, diseñaron y sentaron las bases para el desarrollo de esas tecnologías. Para ello retomamos nuevamente la obra de Paul Ricoeur, *Tiempo y narración,* que parte de la *representación* (no reproducción) de la realidad a partir de la hermenéutica. Para ese autor, la hermenéutica debe partir de la posibilidad de interpretación múltiple tomando en consideración aspectos sociohistóricos tanto de las obras como de sus autores.

El propio Ricoeur enriquece el análisis hermenéutico y por tanto la posibilidad de interpretación a partir de lo que denomina triple mímesis, donde la *mímesis I* consiste en la primera comprensión, haciendo referencia a las experiencias previas, la visión del mundo que permite la existencia de la obra y su autor. La *mímesis II* se refiere al estado del arte de la obra y sus relaciones entre el autor, la obra y su contexto. La *mímesis III* consiste en relacionar al objeto de estudio con la realidad y en la interpretación propiamente dicha. (Ricoeur, 2004).

De esa manera, precisamos aquí los procesos sociales de comunicación

contemporáneos, que alternan la mediación dialógica con la mediación tecnológica, están profundamente ligados a las obras de Turing y de Shannon, quienes desarrollaron tanto los basamentos científicos como los principios operativos fundamentales de la comunicación secreta y las TIC, aspectos que abordamos a profundidad en los capítulos II, IV y V de este trabajo. Así, reiteramos, como Turing concibe y construye métodos matemáticos para cifrar y descifrar códigos y mensajes y para almacenar y transmitir todo tipo de información mediante principios análogos a la comunicación humana, es decir, mediante formas de inteligencia artificial, Shannon sienta las bases de la teoría convencional de la comunicación, generando un modelo matemático que permite formalizar cuando menos un aspecto mecánico de la transmisión/recepción de señales en determinados entornos electromagnéticos.[23]

I.2. La hermenéutica profunda, herramienta principal de análisis

En "La metodología de la interpretación", (en *Ideología y cultura moderna*) John B. Thompson intenta examinar la división entre la discusión teórica y el análisis práctico y explorar algunos de los vínculos existentes entre los debates teóricos que se dan en torno a la cultura, la ideología y la comunicación de masas, por una parte, y el análisis práctico de las formas simbólicas por la otra, a partir del marco metodológico que denomina *hermenéutica profunda*. Ahí pretende "demostrar que ésta proporciona un marco en el cual se pueden interrelacionar de manera sistemática diferentes métodos de análisis, así como apreciar sus ventajas y límites; se adapta con facilidad para analizar la ideología y la comunicación de masas, (Thompson, 2002, p. 399) ya que proporciona un marco metodológico general. Aunque la tradición hermenéutica tiene sus orígenes en la Grecia clásica, los desarrollos asociados con el trabajo de los filósofos hermenéuticos de los siglos XIX y XX como Dilthey, Heidegger, Gadamer y Ricoeur, tienen una

[23] El periodo en el que Turing y Shannon trabajan, que coincide con las aportaciones de científicos de la talla de Wiener y Rosenblueth, ocurre en el momento histórico singular, en cual literalmente se puso en juego la supervivencia de la humanidad, el de la Segunda Guerra Mundial.

relevancia particular por lo que se toman en cuenta en esta investigación.[24]

Si bien en la tradición hermenéutica, muchos fenómenos son formas simbólicas que suscitan problemas de comprensión e interpretación, en las ciencias sociales "el objeto de nuestras investigaciones es en sí mismo un campo preinterpretado", explica Thompson. Por tanto, "El mundo sociohistórico no es sólo un campo-objeto que está allí para ser observado; también es un campo-sujeto constituido, en parte, de sujetos que, en el curso rutinario de sus vidas diarias, participan constantemente en la comprensión de sí mismos y de los demás, y en la interpretación de las acciones, expresiones y sucesos que ocurren en torno a ellos."

También con Thompson aludimos al trabajo de Heidegger, quien "…ha sacado a relucir la importancia de considerar el proceso de comprensión, no como un procedimiento especializado empleado por el analista en la esfera sociohistórica, sino más bien como una característica fundamental de los seres humanos en cuanto tales: comprender es algo que nosotros, en tanto seres humanos, hacemos todo el tiempo de todas maneras, y los procedimientos de interpretación más especializados que emplean los analistas sociales dan por sentadas las bases preestablecidas de la comprensión cotidiana, y se inspiran en ellas".[25]

De esa manera "…Los analistas [sujetos capaces de comprender, reflexionar y actuar a partir de esa comprensión y reflexión] ofrecen la interpretación de una interpretación, reinterpretan un campo preinterpretado; y puede ser importante considerar […] de qué manera se relaciona esta interpretación con las interpretaciones que existen (o existían) entre los sujetos que constituyen el mundo sociohistórico, y cómo puede estar alimentada por ellas" (Thompson, 2002). En consecuencia, debemos tomar en cuenta que todos los seres humanos

[24] Además de las obras citadas anteriormente, de Thompson se utiliza *Hermeneutics: A Study in the Thought of Paul Ricoeur and Jürgen Habermas* (1981).
[25] Véase también Heidegger, Martin, (1951): *Ser y Tiempo,* una de las obras más importantes de la filosofía occidental.

somos parte de la historia, que no somos simples observadores o espectadores de ella y que las tradiciones históricas y los complejos conjuntos de significado y valor que se transmiten de generación en generación, son constitutivos fundamentales de lo que somos.

Por su parte, Gadamer concibe la *comprensión* como una fusión de horizontes históricos, como una producción creativa de significado que aprovecha implícitamente los recursos de las tradiciones. Él mismo pone especial atención al hecho de que " …los seres humanos forman siempre parte de contextos sociohistóricos más amplios y que el proceso de comprensión es siempre algo más que un encuentro aislado entre varias mentes. Siguiendo a Gadamer, Thompson lo llama la " historicidad de la experiencia humana"; la experiencia nueva siempre se compara con el pasado; construimos siempre sobre lo ya presente. (Thompson 2002*:* 401 y Gadamer 1975: 235-274).[26]

Por otro lado, Ricoeur (1969), a partir de Heidegger, del propio Gadamer y de Jürgen Habermas[27], busca demostrar que la hermenéutica puede ofrecer reflexión filosófica acerca del ser y comprender, y reflexión metodológica acerca de la naturaleza y las tareas de la interpretación en la investigación social; lo que ha llamado hermenéutica profunda y es nuestro punto de partida y del mismo Thompson. Este último enriquece el debate al explicar que el proceso de interpretación puede ser y exige ser mediado por una gama de métodos explicativos u objetivantes.

Así, la explicación e interpretación se tornan en momentos complementarios (no excluyentes) en una teoría interpretativa comprehensiva, como pasos que se

[26] Cita de Marx y Engels, 18 Brumario: "…en tiempos de conflicto y cambio social rápidos, los seres humanos tienden a "conjurar a los espíritus del pasado" a fin de disfrazar el presente y reasegurar su continuidad con el pasado" (en Thompson, 2002, 402).

[27] En sus *Essais d'herméneutique* Paul Ricoeur (1969) propone una "hermenéutica de la distancia"; se interpreta a partir de una distancia entre el emisor y el receptor. Al mismo tiempo este discurso cobra independencia y se encuentra desligado del emisor. Pero esta misma realidad propone un "yo" que debe ser extraído por el lector en la tarea hermenéutica. Así, uno de los ejes de la teoría de Paul Ricoeur es la reelaboración del texto por parte del lector.

apoyan mutuamente en un "marco hermenéutico único"[28] Pero, además, dentro del enfoque de la hermenéutica profunda, el punto de partida primordial e inevitable es la hermenéutica de la vida cotidiana, que debe basarse, en lo posible, en una elucidación de las maneras en que las formas simbólicas[29] son interpretadas y comprendidas por los individuos que las producen y las reciben en el curso de sus vidas diarias. Este momento etnográfico es un prerequisito eliminar indispensable para el enfoque de la hermenéutica profunda. "Por supuesto, semejante reconstrucción constituye en sí un proceso interpretativo; es una interpretación de la comprensión cotidiana o […] una interpretación de las doxas[30], una interpretación de las opiniones, creencias y juicios que sostienen y comparten los individuos que conforman el mundo social"[31].

En este sentido, una condición hermenéutica fundamental de la investigación sociohistórica es analizar **las formas simbólicas** en "los contextos en que se producen y son recibidas por los individuos que de manera rutinaria extraen sentido de ellas y las integran a otros aspectos de su vida. […] es decir, que el campo-objeto de la investigación debe ser también el campo-sujeto en el que las formas simbólicas son preinterpretadas por los sujetos que constituyen este campo" (Thompson, 2002: 406-407).

Thompson realiza una ruptura metodológica con la hermenéutica de la vida diaria, que se basa exclusivamente en la interpretación de las doxas pues hay que ir más allá y acudir al marco metodológico de la hermenéutica profunda, basada en tres dimensiones analíticamente distintas dentro del proceso interpretativo:1) **Ámbito**

[28] Para Ricœur, el objetivo de la hermenéutica es recuperar y restaurar el significado. El filósofo francés elige el modelo de la fenomenología de la religión, en relación con el psicoanálisis, destacando que se caracteriza por una preocupación sobre el objeto.

[29] Las formas simbólicas son unidades (puede ser cualquier tipo de acción, objeto o expresión, no necesariamente un producto mediático) que en su conjunto conforman la cultura (el todo) de las sociedades

[30] En Platón, las doxas se relacionaban con la experiencia y la opinión; funcionan como motivaciones que parecen naturales e inherentes a cualquier actividad social humana. El término doxa aparece también en la teoría de Pierre Bourdieu sobre los campos, para hablar de las ideologías que ya no son cuestionadas y que forman parte fundamental de un campo.

[31] La interpretación de las doxas se basa en obras filosóficas de Wittgenstein; escritos fenomenológicos de Husserl y Schutz y el enfoque etnometodológico de Garfinkel, Cicourel y otros en el significado metodológico de su interpretación.

espacio-temporal: reconstrucción de los lugares en que se producen y reciben (en nuestro caso, los primeros sesenta años del siglo XX en Europa, particularmente en Inglaterra, y en América, en Estados Unidos); 2) **Campos de interacción específicos**: como un espacio de posiciones y conjunto de trayectorias que determinan ciertas relaciones que se dan entre los individuos (Turing y Shannon ante los paradigmas científicos y el desarrollo de la criptografía del momento ante la Guerra), y 3) **Análisis sociohistórico** a través de las instituciones sociales (conjuntos relativamente estables con reglas y recursos aunados a las relaciones sociales, que dan una forma particular a los campos de interacción) distintas a la estructura social. Turing y Shannon ante las problemáticas inherentes al desarrollo de la guerra.

Así, en esta investigación se toman en cuenta de manera general los escenarios espacio-temporales, los campos de interacción, las instituciones sociales, la estructura social y los medios técnicos de transmisión que correspondieron a Turing y a Shannon pues "La tarea de la primera fase del enfoque hermenéutico profundo es reconstruir las condiciones sociohistóricas y los contextos de producción, circulación y recepción de las formas simbólicas, así como las reglas y convenciones, las relaciones e instituciones sociales, y la distribución del poder, los recursos y las oportunidades en virtud de los cuales estos contextos forman campos diferenciados y socialmente estructurados" (Thompson, 2002: 412).

Dado que escapa a los objetivos de esta investigación y que en la primera fase del análisis delimitamos el contexto sociohistórico, no profundizamos en la segunda fase, el análisis formal o discursivo (que se refiere al análisis de los rasgos estructurales y de las relaciones de discurso), ni en el análisis semiótico (abstracción metodológica que estudia maneras en las que los elementos se combinan para decir algo acerca de algo, paso parcial en un procedimiento interpretativo más comprehensivo).

Tampoco nos centramos en los métodos del análisis discursivo, que comprenden

al análisis conversacional (Harvey Sacks y Emanuel Schegloff) las propiedades sistemáticas de formas de interacción lingüística; el análisis sintáctico (de la gramática o sintaxis operativa); el análisis de la estructura narrativa[32] ni el análisis argumentativo (reconstruir y hacer explícitos los patrones de inferencia que caracterizan al discurso). Todo ello se dejó fuera de nuestra investigación dado que rebasa los límites propuestos para este trabajo.

En cambio, con Thompson, partimos de que interpretación y reinterpretación "…proceden del análisis: examinan, separan, deconstruyen, buscan develar los patrones y recursos que constituyen una forma simbólica o discursiva, y que operan en ella". Nuestra interpretación se construye, pues, sobre este análisis y sobre los resultados del análisis sociohistórico, tomando en cuenta que "…la interpretación implica un nuevo movimiento del pensamiento: procede por síntesis, por la construcción creativa de un significado posible". Así, nuestro marco metodológico basado en la hermenéutica profunda nos permitió apreciar métodos de análisis, como el sociohistórico y acotar sus límites: "Se trata de un patrón intelectual para un movimiento de pensamiento que investiga los rasgos distintivos de las formas simbólicas sin caer en las trampas gemelas del internalismo o el reduccionismo". (Thompson, 2002: 420-423).

Con el académico colombiano Daniel Herrera Restrepo tomamos en cuenta el punto de encuentro entre fenomenología[33] y hermenéutica a partir de la visión

[32] Por ejemplo en Propp y el cuento ruso, Roland Bartres, Levi-Strauss, Greimas, Todorov y Genette con respecto a la historia como constelación de personajes y sucesión de hechos.

[33] La fenomenología se refiere al estudio de los diferentes modos en que las cosas aparecen o se manifiestan en la conciencia. Esta corriente idealista subjetiva -cuyo posterior movimiento filosófico del siglo (escuela fenomenológica) se debe, entre otros, a E. Husserl quien siguió a los neo-kantianos alemanes de fines del siglo XIX en especial W. Dilthey- describe las estructuras de la experiencia tal y como se presentan en la conciencia, sin recurrir a teoría, deducción o suposiciones procedentes de otras disciplinas. La fenomenología parte del concepto central de la `intencionalidad de la conciencia' que trata de fundamentar que no hay `objeto sin sujeto'. Presta atención a los objetos ideales, universales y temporales, que no pueden existir materialmente (reducciones fenomenológicas) para aprehender las esencias de la conciencia pura, en un proceso en que la inducción desempeña su papel vital. Los requisitos básicos de esta doctrina se observan en la reducción fenomenológica o tendencia a abstenerse de formular juicios que conciernen a la realidad objetiva y que rebasan los límites de la experiencia pura (subjetiva). Pretende estudiar las esencias de las cosas y la de las emociones.

husserliana de mundo de vida, pero en ello tampoco profundizamos en este trabajo.[34] Partimos, pues, de que la hermenéutica[35] es el conocimiento y arte de la interpretación, para determinar el significado exacto de las palabras mediante las cuales se ha expresado un pensamiento. Pasamos después a objetivar las fases o procedimientos principales que comprenden a la hermenéutica profunda; es decir, las dimensiones analíticamente distintas del proceso interpretativo, a partir del análisis sociohistórico y de la Interpretación/reinterpretación.

I.3. En nuestro siglo XX (espacio y tiempo)

Desde el inicio de esta investigación partimos de que el "…mundo sociohistórico no es sólo un campo-objeto que esté allí para ser observado; también es un *campo-sujeto* constituido, en parte, de sujetos que en el curso rutinario de sus vidas diarias participan constantemente en la comprensión de sí mismos y de los demás, y en la interpretación de las acciones, expresiones y sucesos que ocurren en torno a ellos". (Thompson, 2002: 399).

Para referirnos a nuestra particular caracterización del siglo XX y centrarnos en los primeros 54 años de ese siglo, año en el cual murió Alan Turing, retomamos al académico Carlos Antonio Aguirre Rojas quien está convencido de que, "desde una perspectiva rigurosamente histórica, los siglos cronológicos, de perfectos cien años, carecen totalmente de relevancia y de interés para los historiadores… Porque la noción de temporalidad en que se apoya la determinación de estos

[34] Véanse los escritos sobre fenomenología de Daniel Herrera Restrepo (1986). Este académico formula, en forma de tesis, los tres aportes que Husserl ha dado a la actual hermenéutica: "1) El sentido y significado de un hecho, de una realidad o de una palabra están predeterminados por su horizonte de donación; 2) Lo presupuesto como "suelo" de toda experiencia y horizonte de todo "darse" con sentido, es el mundo de la vida cotidiana (Lebenswelt); 3) Todo comprender, científico o no científico, presupone una "precomprensión" del mundo, articulada de antemano lingüísticamente".

[35] Hay varios acercamientos hermenéuticos dignos de mención. Destacan los de la hermenéutica filológica, surgida en Alejandría para establecer el sentido auténtico de los textos antiguos, y particularmente los grandes poemas de Homero. Siglos más tarde, filólogos influidos por el Idealismo alemán y sobre todo Leo Spitzer, propusieron un nuevo método de interpretación de los textos mediante la estilística y el círculo filológico, la hermenéutica bíblica. Intenta trazar un puente de comprensión entre el pasaje bíblico (palabra escrita) y la realidad presente. Por otra parte, la hermenéutica filosófica es independiente de la lingüística y busca determinar las condiciones trascendentales de toda interpretación. Es decir, interpreta las actividades del hombre culto. Véase Diccionario Filosófico

siglos pur amente c ronológicos es una n oción d emasiado l imitada frente a l as exigencias y a la complejidad que el verdadero análisis histórico reclama".[36]

Alejándonos pues de la caracterización del tiempo y del espacio como algo lineal, los abor damos c omo " un t iempo s ocial-histórico c ompuesto por m últiples duraciones, t iempo q ue es c omplejo, di verso, v ariable –en c uanto a s us r itmos, densidades, medidas, c ortes, dur aciones y ar ticulaciones diversas–, s iendo además un tiempo que, en rigor, se encuentra cortado a la medida de los mismos hechos, fenómenos y pr ocesos s ociales q ue, t anto l os c ientíficos sociales c omo los seguidores de Clío estudian y analizan cotidianamente".[37]

Con el r econocido h istoriador E ric H obsbawm[38] y e l m ismo Aguirre Rojas retomamos la historia del siglo XX con cortes trascendentes como las dos guerras mundiales p ues s i al go l o c aracteriza " …es l a de es a v iolencia des enfrenada, irracional, c reciente y absurda, de 1914-18, del hol ocausto j udío, de l a s egunda guerra mundial, pero también de la guerra en contra de Vietnam, de las masacres de las dictaduras y los gobiernos de A mérica Latina, África y Asia, de las guerras étnicas f ratricidas de Ruanda y de Kosovo…" (Aguirre R ojas, 2004: 47). Porque "…es c laro q ue l a pr imera y l a s egunda g uerras m undiales, p ero t ambién e l fascismo, el naz ismo y el f ranquismo, c onstituyen v arios de l os es labones centrales de u na c lara *regresión* de la c ivilización c apitalista e n lo q ue t oca a l desarrollo de l os m ecanismos de au tocontrol de l os i mpulsos violentos, y al establecimiento del Estado como detentor del monopolio exclusivo de la violencia legítima".[39]

[36] Véase el capítulo 1, Balance crítico del siglo XX histórico. ¿Breve, largo o muy largo siglo XX?", de *Para comprender el siglo XXI,* Ediciones de Intervención Cultural/*El viejo topo*, España, 2005: 26.

[37] El tiempo histórico social parte de la corriente historiográfica francesa de la llamada Escuela de *Los Annales*. Véase también Marc Bloch, *Apología para la historia o el oficio del historiador*, FCE, México, 1996 y Braudel, Fernand, *Escritos sobre historia*, FCE, México, 1991. (Aguirre Rojas, Carlos Antonio, 2004: 26-27).

[38] Véase el excelente y completo texto de Eric Hobsbawm y su Historia del siglo XX, 1994, que la describe como historia corta, de la Primera Guerra Mundial a la caída del muro de Berlín.

[39] Consúltese a un estudioso de esos procesos: Elias, Norbert, *El proceso de civilización*, FCE, México, 1989; también en *Los alemanes*, Instituto Mora, México, 1999, explica a profundidad el holocausto judío.

Más allá de si tratamos al siglo XX como un siglo corto o largo, nos inclinamos por la idea de lo que han hecho, a decir de Aguirre Rojas, los historiadores y científicos sociales realmente críticos: "…establecer, muy claramente, que la *específica duración* de cada siglo histórico depende, esencialmente, de los principales procesos y fenómenos históricos que lo caracterizan y que dentro de él se despliegan, que con su propia curva o itinerario de vida global determinan justamente esos cortes iniciales y terminales de cada siglo histórico estudiado". (Aguirre Rojas, 2004: 27).

Así, al tratar de caracterizar la temporalidad específica del siglo XX histórico y cuáles han sido los procesos y fenómenos fundamentales que han ocurrido, abogamos con Aguirre Rojas, por un "breve siglo XX", que comienza hacia 1914 –o en nuestro caso 1912, año del nacimiento de Turing y 1916, el de Shannon– para cerrase hacia 1954 con la muerte del primero. ¿Cuáles han sido entonces los hechos dominantes que caracterizan a nuestro *breve siglo XX*? Sin duda las dos guerras mundiales, las etapas de construcción de la hegemonía estadounidense y capitalista; los movimientos independentistas y socialistas en distintos países; el acelerado avance de la ciencia y el surgimiento de las tecnologías de la información y la comunicación; de las computadoras y la era digital; todos temas que retomamos más adelante.

Partimos, reiteramos, de un muy corto siglo XX, que cronológicamente comenzamos en 1912 y terminamos en 1954 y en el que se toman en cuenta acontecimientos relevantes, siempre en consideración —como explica Marc Bloch en su *Apología para la historia o el oficio del historiador, 1941-1943*— de que "La verdadera exactitud consiste en dejarse guiar, en cada ocasión, por la naturaleza del fenómeno considerado". *(*Aguirre Rojas 2004, 38*).*

En el marco de entender desde H.G. Gadamer en *Truth and Method* y en Eric Hobsbawm que la experiencia humana es siempre histórica, que los sujetos se

insertan siempre en tradiciones históricas, comenzamos con el entorno inmediato tanto de Turing como de Shannon (nuestros *fenómenos* considerados).

I.4. En dos mentes, un tiempo y dos espacios

En nuestro caso particular, la dimensión analítica del estudio sociohistórico no podría avanzar sin la ubicación geográfica en el **tiempo** y el **espacio** en el que vivieron Turing y Shannon. El británico Alan Mathison Turing (1912-1954) es uno de los científicos más reconocidos por sus aportaciones a distintas áreas de la ciencia; sobre todo en las matemáticas y la computación.[40]

Incluso Turing ha sido calificado como una de las mentes más creativas y geniales en la historia de la humanidad por reconocidos historiadores de la ciencia y medios como la revista *Time* que al publicar una relación con las 100 más grandes mentes del siglo XX, aparecía Turing, junto a Einstein, los descifradores del ADN, Crick y Watson, y el descubridor de la penicilina, Alexander Fleming. Además de ser un destacado matemático y estudioso de la lógica, sus trabajos de investigación desarrollados en la primera mitad del siglo XX, y específicamente su artículo sobre los números computables, permitieron el surgimiento de las actuales tecnologías o plataformas sobre las que operan Internet, las redes digitales y en general todo lo relativo a sistemas de cómputo electrónico. [41]

Como lo acotamos anteriormente, mediante sus investigaciones secretas (que vemos en el capítulo VI de esta investigación) y su afán por romper esquemas y traspasar límites tanto en su trabajo teórico como en su vida personal[42], Turing se adelantó a su tiempo al desarrollar teorías, instrumentos y máquinas de decodificación del lenguaje, que darían pie no sólo a acelerar el término de la Segunda Guerra Mundial con el triunfo de los Aliados sino también a las bases de lo que hoy son la comunicación secreta, la computación, la inteligencia artificial y a

[40] Como acotamos, son varios los biógrafos de Turing; entre los más importantes están Andrew Hodges, (2000) y David Leavitt (2006).
[41] Véase también la revista *Ciencia* (oct-dic. 2013) de la AMC sobre Alan Turing y la computación y la revista *Temas de IyC* (Abril/Junio 2012), *La ciencia después de Alan Turing*, un monográfico sobre su vida y obra.
[42] Véase el artículo de Valek, G. (2012) "Alan Mathison Turing: explorador de límites".

las TIC, parte esencial del mundo actual. Por tanto, y lo reiteramos, este científico, al que se ignora en los estudios de comunicación, debería ser uno de los pilares de nuestro bagaje teórico.

Por su parte, recapitulamos, Shannon (1916-2001) cambió nuestra percepción de la información a l demostrar con su artículo "Una teoría matemática de la comunicación", que la información[43] podía definirse y medirse como una noción científica y que los dígitos binarios eran sus elementos fundamentales. Con ese texto nació la teoría de la información, que abarca desde aplicaciones abstractas en áreas que van de la biología a la lingüística, pasando por la termodinámica y la física cuántica, hasta la computación y otras disciplinas de esencia matemática, basadas en conceptos como el de capacidad de un canal de transmisión. Su interés se centró en aspectos técnicos, pero también hizo importantes contribuciones a otros campos como la criptografía, la inteligencia artificial y las telecomunicaciones.[44] Además de su famoso "A Mathematical Theory of Communication", publicado en *Bell System Technical Journal*, en julio de 1948, de Shannon, retomamos más adelante un texto ya desclasificado (que se mantuvo secreto incluso años después en la posguerra) sobre la teoría del criptoanálisis.[45]

I.5. En las categorías de la comunicación secreta y de la criptografía computacional

Aplicar la teoría de la interpretación en la criptografía computacional resultó una estrategia metodológica enriquecedora para nuestro proceso de investigación puesto que, pese a su importancia en las TIC, en los medios de comunicación e

[43] Si bien el debate entre información y comunicación ha sido superado, vale la pena referir el texto de A y M. Mattelart, *Historia de las teorías de la comunicación*, editorial Paidós, México, 1997. Por lo pronto, diremos que los objetivos de la información son transmitir los datos necesarios para la toma de decisiones. Los procesos de comunicación, en cambio, son más amplios pues implican una relación social que permite la amplia interacción humana. Los pasos básicos de ambas son la intención de informar o comunicar, la composición del mensaje, la claridad e inteligibilidad del mismo, la codificación del mensaje, la transmisión y recepción de la señal, la decodificación del mensaje y la interpretación del mensaje por parte de un receptor.

[44] De las biografías de Shannon tomamos a varios historiadores de la ciencia y académicos de la computación.

[45] Otros autores, como Abrahan Sinkov (2009)y su "Elementary Cryptanalysis," y Jacob, Odile (1998) en *La Science du*, aportan elementos importantes al análisis.

incluso en nuestra vida cotidiana, la criptografía computacional es un campo ignorado desde nuestra área disciplinaria de las ciencias de la comunicación. Aunque en el capítulo V relacionamos los antecedentes históricos de la criptografía computacional y su importancia en las TIC y para las ciencias de la comunicación, nos detuvimos en la Segunda Guerra Mundial, etapa generadora de trascendentes cambios y crucial en la historia de nuestros personajes y, nos atrevemos a afirmar, de la humanidad.

Tomamos a la criptografía como el modo específico (especializado e instrumental) de semiótica, entendiendo por semiosis (o criptografía) la capacidad de generar códigos de operación (cadenas lógicas de enunciados) que significuen (representen) algo. Omitimos por ahora las distintas corrientes de estudio y teorías de la comunicación que ya han sido ampliamente estudiadas por científicos sociales y las retomamos en el capítulo III, donde vamos del modelo de Lasswell a la noción del "actuar comunicativo" de Jüngen Habermas, por mencionar sólo las más importantes[46]. Nos centramos, en cambio, en otros aspectos, que consideramos de gran trascendencia comunicativa, que han sido poco explorados pero pertenecen a un importante campo disciplinario que cada vez está tomando más fuerza y que en esta investigación denominamos "comunicación privada o **comunicación secreta.**[47]

Por una parte, con el contexto sociohistórico analizamos (interpretamos) cómo, con otros matemáticos e ingenieros de su generación, Alan Turing hizo posible el desarrollo y utilización de máquinas *computables* para cifrar, enviar, recibir y descifrar mensajes privados (secretos). Para el análisis posterior sólo mencionamos algunos de los más importante documentos y artículos de Turing, entre los que se encuentran los que dieron pauta a lo que hoy conocemos como ciencias de la computación.[48]

[46] A algunas de ellas, como el modelo de Lasswell, nos acercamos en futuros momentos del análisis.
[47] Véase Flores Morador, Fernando, (2003): "Lo humano y lo artificial en la comunicación electrónica".
[48] Se trata de "On Computable Numbers" y "Mechanical Intelligence", textos importantes pero demasiado técnicos y especializados para nuestros objetivos de investigación. Otros de sus trabajos y documentos

Para enmarcar este análisis, de todas las teorías o modelos de estudio de las ciencias de la comunicación, nos centramos en la teoría matemática de la información de Shannon (que, como es sabido, fue conocida posteriormente como de Shannon-Weaver[49]) y de la premisa de que, al ser sobre todo un modelo matemático, no alcanza a abarcar (ni le interesaba hacerlo) el análisis ampliamente comunicativo; no explica qué ocurre cuando el mensaje es indescifrable (ya sea por carecerse de la clave o llave para descifrarlo) y después por ser demasiado complejo al estar codificado y requerir de una máquina que lo descifre. Muchas de las aportaciones de Shannon se tomaron de sus biógrafos pero también de entrevistas y documentos originales, particularmente dentro de los Laboratorios Bell, donde trabajó durante los años que concernieron a esta investigación.[50]

La contribución de Turing y Shannon consistió en haber sido capaces –desde sus propias trincheras– de concebir la noción de información, descifrarla y manipularla para reproducirla primero mecánicamente y después de manera electrónica pero no debemos perder la objetividad y perspectiva. Estamos de acuerdo con Fernando Flores Morador en que "La fascinación que este logro ha generado nos ha llevado a excesos nada distintos de aquellos que todo gran logro genera en la mente del hombre. Observando el impacto ideológico que la computación moderna ha tenido en nuestro tiempo, podemos representarnos el impacto que

---

fueron posteriormente agrupados en el texto *The Essential Turing: The Ideas That Gave Birth to the Computer Age*, editado por B. Jack Copeland y publicado por Oxford University Press. Los textos completos de Turing se encuentran en cuatro volúmenes en *Collected Works* of A. M. Turing, publicado por North-Holland. Algunos de los documentos originales de Turing y que tuvimos la oportunidad de analizar en una práctica de campo en mayo-junio de 2018 se encuentran en el Kings College de la Universidad de Cambridge y pueden consultarse en línea en http://www.turingarchive.org.

[49] Como ya dijimos, Warren Weaver (1894-1978) consiguió dar mayor alcance al planteamiento inicial de Shannon, que se restringía a la transmisión de estos mensajes.

[50] Shannon pasó quince años en los Laboratorios Bell con destacados matemáticos y científicos como los inventores del transistor; George Stibitz, quien construyó computadoras basadas en relés o relevadores, dispositivos electromecánicos que funcionan como interruptores controlados por un circuito eléctrico en el que, por medio de una bobina y un electroimán, se acciona un juego de uno o varios contactos que permiten abrir o cerrar otros circuitos eléctricos independientes. Ahí conoció también al propio Warren Weaver, su coautor en *Una teoría matemática de la comunicación* y a muchos otros más.

otrora tuvo la imagen pintada en las cavernas prehistóricas, o el de la palabra escrita en los albores de la civilización" (Flores Morador, 2003).

Así, **de la misma manera en que Alan Turing construye una serie de procesos matemáticos que apuntan al uso de mecanismos electrónicos para cifrar y descifrar códigos y mensajes y almacenar y transmitir información mediante principios análogos a la comunicación humana (formas de lo que podría considerarse hoy inteligencia artificial), Shannon postula las bases de la teoría convencional de la comunicación, con un modelo matemático que permite formalizar un aspecto mecánico de la transmisión/recepción de señales en entornos electromagnéticos**.[51]

Como lo vamos sustentando en esta investigación, nuestra premisa fundamental es que las TIC de hoy no serían posibles sin el trabajo teórico (*máquina de Turing e inteligencia artificial*) que desarrolló el matemático y filósofo británico en las primeras décadas de l siglo XX, ni tampoco sin la Teoría matemática de la información, desarrollada por el matemático e ingeniero estadounidense**,** que darían pie a las computadoras electrónicas.

I.6. En la categoría de las tecnologías de la información y la comunicación

En términos generales retomamos la definición de las tecnologías de la información y comunicación como aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información. La tecnología de la información se encuentra generalmente asociada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones. (Bologna y Walsh, 1997).

Como hemos acotado, las TIC, a las que tomamos por lo pronto como " toda transmisión, emisión o recepción, incluido el procesamiento, de signos, señales,

[51] Nuestro análisis también toma en cuenta la analogía entre las aportaciones sobre codificación y criptografía planteadas en la Teoría matemática de la información de Shannon (1948) y las aportaciones de Turing en cuanto al desarrollo de la criptografía computacional (a partir de su artículo "Maquinaria computacional e inteligencia", de 1950).

escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos"[52] son hoy parte fundamental de nuestra vida no sólo cotidiana sino dentro de nuestro campo de acción y estudio, en las ciencias de la comunicación.

Si bien sus orígenes y desarrollo han sido explorados por distintas áreas científicas y específicamente desde las teorías matemáticas de la información y la computación, poco se ha hecho desde las ciencias sociales para entender el contexto y momento coyuntural en el cual surgieron sus pioneros y las ideas que dieron pie y origen a lo que hoy conocemos como TIC.

Aunque sí contamos con importantes estudios sobre sus orígenes y desarrollo en nuestras sociedades particulares[53], poco se ha estudiado, desde la comunicación, sobre aquellos personajes de la ciencia que les dieron origen y a quienes hoy debemos innumerables aplicaciones. Dos de esos pioneros son Alan M. Turing y Claude E. Shannon. El primero ha sido completamente ignorado y, como vemos más adelante, al segundo se le ha criticado por no centrarse en los contenidos comunicativos y ceñirse solamente al fenómeno de transmisión de la información.

Una vez delimitada en el presente capítulo la estrategia metodológica de análisis que rige este trabajo de investigación y establecidas nuestras principales categorías, así como la conexión a desarrollar desde la hermenéutica profunda, en el capítulo II ubicamos sociohistóricamente a Turing y a Shannon en el contexto que les tocó vivir y que ellos mismos transformaron.

Más adelante, en el capítulo III de esta investigación nos referimos a los principales modelos de la comunicación y a la omisión total de Turing y parcial de Shannon en las escuelas de comunicación para seguir en el capítulo IV con el desarrollo de las TIC en el contexto sociohistórico del siglo XX y en la criptografía

[52] UIT, 2012 en Alva de la Selva 2015 41.
[53] Véase, por ejemplo, el texto de Alva de la Selva 2015, que se refiere particularmente a México.

computacional y en la comunicación secreta en tiempos de guerra en el capítulo V.

En el último capítulo de este trabajo (el VI) se ubican a Turing y a Shannon en las ciencias de la comunicación a partir de sus aportaciones a la comunicación secreta y a la criptografía computacional y se propone cómo incorporarlos ampliamente a los proyectos de investigación y programas de estudio de nuestra disciplina.

Capítulo II
El contexto sociohistórico en los primeros sesenta años del siglo XX alrededor de Alan M. Turing y Claude E. Shannon

"Creemos con Hegel que una época no se caracteriza solamente por su modo de actuar, sino también por su cultura y modo de pensar, por su arte, su ciencia y su filosofía"[54]

Una vez explicada la estrategia metodológica de análisis, en este capítulo abordamos lo referente al contexto histórico general y científico particular de los primeros sesenta años del siglo XX en el mundo occidental desde la hermenéutica profunda[55]. Aquí cabe reiterar que tomamos sólo un poco más de los primeros cincuenta años del siglo XX en función del tiempo de vida de uno de los dos personajes centrales de este trabajo de investigación, el británico Alan M. Turing, quien vivió de 1912 a 1954. Aunque el estadounidense Claude E. Shannon lo hizo de 1916 a 2002, ya en otro siglo, sus principales aportaciones a la criptografía ocurrieron también en los primeros 60 años del siglo pasado.

Dentro del contexto histórico, se plantea la construcción del concepto de las TIC para ir acercándonos a la criptografía computacional y a la comunicación secreta y en los nuevos medios para dar pie posteriormente, en el capítulo IV, a su desarrollo específico. (Manovich 2005).

II. 1. El contexto

Alan Mathison Turing nació en la capital de la Inglaterra imperial el 23 de junio de 1912, dos años antes de que estallara la Primera Guerra Mundial (1914-1918) y cambiara drásticamente el panorama político, económico y social del planeta. La infancia de Turing fue distinta a la de la mayoría de los niños ingleses de su tiempo pues estuvo dividida entre la India y el Reino Unido. Sus padres vivían en

[54] Véase *El legado filosófico y científico del siglo XX* de Manuel Luis M. Valdés y Luis Arenas (2005, 19).
[55] Véase, entre otros, Ferraris, Maurizio (1999 y 2002).

la entonces colonia británica cuando lo concibieron y ellos y su hermano mayor viajaron a Inglaterra para su nacimiento. Su vida y su obra estarían marcadas por esa dualidad y un profundo sentido de pérdida y decadencia del mperio británico (Valek, 2012).

Claude Elwood Shannon, por su parte, nació cuatro años después que Turing, el 30 de abril de 1916, en Petoskey, Michigan, una pequeña ciudad del noreste de Estados Unidos donde, pese al ambiente bélico de la Primera Guerra Mundial, pasó una infancia tranquila y con un enorme sentido de esperanza y prosperidad. Ambos se conocerían décadas más tarde, en el contexto de otra confrontación bélica, la Segunda Guerra Mundial (1939-1945) y desde las matemáticas y la lógica, en el caso de Turing y la ingeniería, en el de Shannon, aportarían su genialidad al futuro desarrollo de la ciencia y la tecnología y de lo que son hoy en día.

Veamos el contexto en el que ambos vivieron y comencemos con un breve recorrido sobre el desarrollo de las ideas en el mundo occidental para hacerlo después brevemente en los campos de la ciencia, la tecnología y la política pues "Así como la hermenéutica nos recuerda que el campo-objeto de la investigación social es al mismo tiempo un campo-sujeto, también nos recuerda que los sujetos que constituyen el campo-objeto son, como los propios analistas sociales, sujetos capaces de comprender, reflexionar y actuar a partir de esta comprensión y reflexión". (Thompson, 2002, 400).

II.2 Las ideas

Con base en la división del *corto siglo XX* planteada anteriormente y que se centra más en hechos relevantes que en fechas, nuestro contexto sociohistórico parte del momento en el cual comienza una centuria marcada por la emergencia de novedosas corrientes filosóficas producto del desarrollo de la ciencia y la tecnología, la política, el desarrollo social y dos guerras mundiales, además de

otros importantes conflictos bélicos regionales más localizados.[56] Entre otros hechos trascendentes se encuentra, por ejemplo, en octubre de 1900, en su obra *La interpretación de los sueños,* Sigmund Freud sienta las bases de la nueva y prometedora ciencia del psicoanálisis. En ella sostiene que los sueños contienen símbolos que revelaban mucho de la personalidad del individuo. Como se apunta en los textos de historia de la psicología[57], su revolucionario trabajo en la sexualidad humana y el poder del inconsciente dio un nuevo significado a las referencias de la libido, el *ego* y el *superego*, con una profunda influencia en el futuro de la cultura moderna que trascendió a lo largo del siglo XX y que tocó ineludiblemente tanto a Turing y a Shannon como a sus contemporáneos.

Pocos años más tarde, en su primera *Memoria* publicada en 1905, sobre la teoría de la relatividad, el físico alemán Albert Einstein propuso una ecuación calificada como la más trascendente del siglo ($E=mc^2$), al demostrar matemáticamente que a las tres dimensiones del espacio físico había que añadirle el concepto del tiempo o cuarta dimensión.[58] De ahí en adelante la ciencia y la tecnología propiciaron cambios drásticos no sólo en esas áreas del conocimiento sino en su inserción en la ciencia, la cultura y vida cotidiana de muchos de los habitantes del planeta; en todo ello tuvo un papel crucial el surgimiento de las TIC, la computadora digital y su masificación, aspectos que vemos con más detalle en los siguientes apartados.

Por considerarlo pertinente para los fines de nuestro trabajo de investigación, específicamente en este capítulo partimos de la –desde nuestro punto de vista– atinada división de la historia de las ideas que hacen Manuel Garrido y otros académicos, en *El legado filosófico y científico del siglo XX*.[59]

---

[56] Éstos han sido explicados detalladamente por el reconocido historiador británico Eric Hobsbawm (1994).

[57] Véase, por ejemplo, Brennan, R. E. *(*1969), Foulquie, P. (1959), y Murphy, G. (1964).

[58] Véase, Stewart, Ian (2015 *17)* donde, con gran sentido del humor y conocimiento del tema, enriquece sus ecuaciones con interesantes y poco conocidas anécdotas que nos acercan a entenderlas y disfrutarlas. Incluye en dichas ecuaciones la de Shannon sobre la Teoría de la información. Véase también la reseña del mismo texto de Valek (I-2016).

[59] Para profundizar al respecto, véase Garrido, Manuel y otros (2005). Recomendamos, particularmente, sus cuadros sintéticos.

Con base en estos autores y siguiendo los lineamientos de la hermenéutica profunda de Thompson (2003, 2010), la primera mitad del siglo XX, puede dividirse en tres momentos temporales del pensamiento filosófico occidental: el primero, de 1901 a 1917; el segundo, de 1918 a 1929 y el tercero, de 1930 a 1945.

De comienzos del siglo XX a 1917 (un año antes del término de la Primera Guerra Mundial), sobresalen cinco corrientes de pensamiento: la fenomenología, el pensamiento analítico, la filosofía de la vida, el pragmatismo y el marxismo, que rompen con la tradición filosófica (neoidealismo kantiano y hegeliano, empirismo positivista) imperante durante las últimas décadas del siglo XIX.

La fenomenología y el movimiento analítico constituyen dos filosofías de diseño científico, impulsadas por las *Investigaciones lógicas* (1900-1901) del filósofo alemán Edmund Husserl (1859-1938) y el británico Bertrand Russell (1872-1970) con sus *Principios de la matemática* (1903). Husserl es el fundador de la fenomenología y Russell, líder –con G. E. Moore (1873-1958)– del movimiento analítico de la Inglaterra de las dos primeras décadas del siglo XX. Ambos compartían la convicción opuesta al positivismo imperante, de la objetividad del pensamiento. (*Garrido, Manuel y otros, 2005, 16-17).*

La filosofía de la vida y el pragmatismo son dos corrientes de impacto popular.[60] La primera muestra diversas tendencias, entre ellas la biologista, estimulada por la revolución científica introducida por Charles Darwin (1809-182) con la teoría científica de la evolución en las ciencias de la vida; la tendencia historicista, con la *Introducción a las ciencias del espíritu* (1883) de Wilhelm Dilthey (1833-1911),

[60] "El pensamiento analítico en su versión russelliana y la fenomenología manejan abundantes tecnicismos y son encuadrables adentro del género llamado por Kant "filosofía académica". La filosofía de la vida y el pragmatismo, tal y como se desarrollan en las primeras décadas del siglo XX, encajan más bien dentro de lo que Kant llamó filosofía popular o "mundana". La filosofía de la vida es, como las dos anteriores corrientes, genuinamente europea. El pragmatismo, que florece de modo paralelo al otro lado del Atlántico, es un producto enteramente *made in USA*", en Garrido, Manuel y otros (2005, 24).

quien de marcó a las ciencias naturales otro he misferio, el de las ciencias del espíritu, cuyo método no es la explicación causal como en la ciencia física, sino lo que él denominó la *comprensión de nexos de sentido*, entre ellos el lingüístico. (*Garrido y otros, 2005*, 26).

Hay otras tendencias, como la vitalista, marcada por el pensamiento de F. Nietzsche (1844-1900), que exhortaba a mirarlo todo y valorarlo desde la óptica o perspectiva de la vida, y Ortega y Gasset (1883-1955) con la frase: "yo soy yo y mi circunstancia", que da cuenta de la inmediata conexión del ser humano con su mundo, la situación sociohistórica en la que vive.

El pragmatismo, por su parte, que se centra más en el mundo de los hechos que de las ideas, tiene al filósofo Charles Sanders Pierce (1839-1914), pionero de la lógica simbólica y de la incorporación del evolucionismo en América, como su principal exponente. En su trabajo *Pragmatismo. Un nuevo nombre para viejas formas de pensar*, William James (1842-1910), otro de sus fundadores, plantea no tomar en cuenta metodológicamente nada que no tenga efectos prácticos.[61]

Otra forma de pensamiento importante en los inicios del siglo XX (y como corolario del Siglo XIX) fue el ascenso del marxismo. Después de la muerte de Karl Marx (1818-1883) " …habían quedado pendientes dos importantes tareas. Una era fundamentar filosóficamente su teoría del materialismo histórico para convertirla en un sistema o concepción acabada del mundo y otra elaborar un plan estratégico que lograse el triunfo de la revolución. Ambas suponían un reto para los múltiples seguidores de Marx y dieron lugar a un prolongado y fértil periodo de creación intelectual en el que se enfrentaron numerosas teorías rivales". *(*Garrido y otros, 2005: 29).

De 1918 a 1929, años entre el término de la Primera Guerra Mundial y cuando ocurre una de las mayores crisis económicas globales, imperan el existencialismo,

[61] Para ampliar esta perspectiva de análisis, véase el citado texto de Garrido y otros (2005).

el pensamiento analítico, el historicismo y vitalismo, el pragmatismo y el marxismo. Años más tarde, de 1930 a 1945, con el estallido de la Segunda Guerra Mundial (1939-1945) sobresalen el existencialismo y la fenomenología, el neopositivismo y la lógica (con Alan Turing como uno de sus principales precursores), la filosofía de la historia, la ontología y el pensamiento moral y político. Todas esas corrientes de pensamiento coexisten en la primera mitad del siglo XX[62] y permean tanto el contexto donde se desarrolla Turing como el que vive Shannon desde la tranquilidad de su hogar estadounidense y los centros de investigación de excelencia en Princeton, Estados Unidos.

II.3 Ciencia, tecnología y política

El siglo XX se caracterizó por grandes avances de la ciencia**,** la tecnología y la medicina en general, pero también por atrocidades humanas globales sin precedentes como varias guerras regionales, continentales y mundiales así como genocidios que cobraron millones de vidas en todas las latitudes y agudizaron las diferencias económicas entre regiones y países.[63]

También el siglo pasado inició en medio de grandes adelantos técnicos e industriales**,** entre ellos, el automóvil y una revolución tecnológica mundial que alcanzó en mayor o menor medida a casi todas las naciones. En algunas prevalecieron los conflictos económicos, políticos y militares. Sólo como ejemplo, tan temprano como en 1905 la guerra ruso-japonesa enfrentó al imperio nipón con el decadente imperio zarista de Rusia, después del ascenso del proletariado, convirtiendo a Japón en una nueva potencia mundial y a Rusia en la Unión de Repúblicas Socialistas Soviéticas.[64] Pero centrémonos en el mundo anglosajón y

[62] Durante la llamada *guerra fría*, de 1946 a 1970, imperarán en el pensamiento anglosajón, la filosofía ciencista, moral y política. En el marxismo, tendencias diversas y la Escuela de Frankfurt. En el pensamiento continental, Alemania y Francia y el pensamiento hispano. Sus principales exponentes se ubican al final de este texto en el citado cuadro 2.

[63] En los últimos años del siglo XX se agudizó el llamado fenómeno de *globalización*, profundas transformaciones económicas globales que no abordaremos aquí pero que vale la pena mencionar y para lo que recomendamos los citados textos de Eric Hobsbawm (1994) y Aguirre Rojas (2004) quienes para comprender el siglo XXI nos explican el XX.

[64] Véase, entre otros Willmott, H.P. (2005) y Basil H. (2001).

en el contexto inmediato que tocó la vida y el desarrollo de las ideas de Turing y de Shannon.

En los primeros años del siglo XX la situación de Alemania dentro de Europa había alcanzado una posición crucial para los intereses de las demás potencias. Al sentirse amenazadas, Gran Bretaña y Francia suscribieron la llamada *Entente Cordiale* para tratar de igualar el desarrollo industrial y militar de Alemania mientras la casa de Austria perdía progresivamente el estatus de gran potencia europea que había mantenido por décadas[65].

En 1914 los conflictos e intereses de las potencias mundiales, dieron pie a la Primera Guerra Mundial que, aunque se inició como un conflicto europeo, terminó involucrando a otras de las principales naciones del orbe. Después de cuatro años de guerra, los principales derrotados fueron los imperios de Austria y Rusia para dar paso a nuevos gobiernos y, en el caso de Rusia, al sistema socialista. Estados Unidos y Japón comenzaron a emerger como potencias mundiales. Alemania perdió su pequeño imperio colonial, pero mantuvo su infraestructura nacional, a diferencia de la destruida Francia, pese haber resultado victoriosa en la guerra. Gran Bretaña, aunque menos afectada que Francia, se encontró en condición de desventaja con Estados Unidos, país sobre el que hacia menos de un siglo aún tenía la pretensión de volver a integrar dentro de sus colonias.

Después del final de la Primera Guerra Mundial, se creó la Sociedad de Naciones**,** que nació con el ideal de evitar que volviese a repetirse un conflicto global. El Imperio Ruso pasó a ser la Unión de Repúblicas Socialistas Soviéticas (URSS) que, con la ideología marxista de Lenin**,** se convirtió en la primera nación del planeta gobernada por la fuerza obrera, el proletariado (Hobsbawm 1994).

[65] Véase en cualquier *Historia Mundial,* los primeros cincuenta años del siglo XX; el libro del divulgador científico Constantino Armestos (1995) donde plantea que conforme avanzó el siglo XX las repercusiones de los avances científicos y tecnológicos sobre la vida cotidiana fueron cada vez más obvios y se produjeron en un tiempo extraordinariamente corto.

Estados Unidos prosiguió un rápido desarrollo económico que se vio alterado, sin embargo, por la *gran depresión* de 1929, que alcanzó efectos mundiales. Alemania, afectada profundamente por las disposiciones establecidas del Tratado de Versalles, tenía su sistema financiero en crisis, mientras trataba de lograr una estabilidad democrática con la República de Weimar bajo la presidencia de von Hindenburg. En Francia había gran descontento social e inestabilidad política.

Adolf Hitler, un político alemán en rápido ascenso, buscaba con el Tercer Reich restaurar la gloria de Alemania y recuperar el territorio que había perdido en la Primera Guerra Mundial. Las primeras conquistas de Hitler se dieron en los pequeños países centroeuropeos de Austria y Checoslovaquia y el 1 de septiembre de 1939 Alemania invadió Polonia, sometiéndola en una semana. Viendo el peligro que entrañaba Hitler para Europa, a los tres días de haberse consumado su ocupación en Polonia, Francia y Gran Bretaña le declararon la guerra y de ahí fueron sumándose varias naciones hasta estallar la Segunda Guerra Mundial. Esta conflagración global se libraría en todos los continentes y provocaría la muerte de millones de personas, no sólo en campos de batalla sino también población civil en las grandes ciudades y en campos de concentración nazi, afectando profundamente la vida social, cultural, científica y económica mundial, particularmente de los países europeos. (Willmott, 2005 y Basil, 2009).

A través de su denominada “Teoría de las razas”, basada en una supuesta supremacía de la raza aria, Hitler promovió el odio hacia judíos, gitanos y otros grupos étnicos y aplicó una política de exterminio masivo. Dentro de esa política de exterminio y segregación, en 1942 puso en marcha la llamada “Solución final” para los once millones de judíos que vivían en Europa: primero tenían que ser trasladados al Este para trabajar y después serían exterminados en campos de concentración como los de Belzac, Treblinka y Auschwitz expresamente creados para ello en territorios alemán y polaco. Hasta comienzos de 1945, cuando Alemania perdió la guerra y se rindió ante los Aliados, en aras de la *solución final* se había *exterminado* a seis millones de judíos.

Independientemente de las graves consecuencias sociales y económicas para la historia de la humanidad y que han sido tratadas en innumerables investigaciones, quizás uno de los ejemplos más importantes sobre el desarrollo científico-tecnológico del momento lo constituya el lanzamiento, el 6 de agosto de 1945, de la primera bomba atómica de la historia, y que se haya hecho sobre una población civil, destruyendo el 60% de la ciudad japonesa de Hiroshima y causando 80 mil muertos y 70 mil heridos de una población original de 330 mil habitantes. Como es sabido, tres días después, el gobierno estadounidense lanzó otra bomba atómica sobre otra ciudad japonesa, Nagasaki, matando a 35 mil de sus 260 mil habitantes. Terminó entonces la Segunda Guerra Mundial, conflagración bélica que tuvo un costo humano sin precedentes para todas las naciones involucradas y el planeta en su totalidad.[66]

II. 4. Alan M. Turing, mente genial

Como señalamos anteriormente, Alan M. Turing nació en Inglaterra y en ese país vivió las dos guerras mundiales. Desde pequeño, fue un niño muy inquieto que dio muestras de genialidad: aprendió a leer por sí mismo en tres semanas; siempre mostró un gran interés por los números y a los 8 años de edad montó un pequeño laboratorio en el sótano de su casa en el que hacía sencillos experimentos. En 1926, a los 14 años de edad, ingresó a un internado en Dorset y en su primer día de clases se hizo famoso en la comunidad ya que apareció en la prensa local: resulta que ese día estalló una huelga general en Inglaterra y, como no había medios de transporte público, Alan recorrió en bicicleta los 97 km que separaban

[66] En Japón, después de muchos años, los sobrevivientes siguieron sufriendo los efectos de la radiación, cáncer de piel, leucemias y malformaciones genéticas. La URSS, que había sido aliada de los países que derrotaron a Alemania y las demás naciones del Eje, se transformó en el "enemigo de occidente" y se dio paso a lo que se conoció posteriormente como ***guerra fría*****,** sobre todo entre Estados Unidos y la URSS. Poco después del fin del conflicto mundial, **China** sufrió una guerra civil y se instaló un régimen totalitario **comunista,** la República Popular China. En la década de 1950, la disputa entre los dos nuevos ejes mundiales, se intensificó con la **guerra de Corea** y la posterior división de ese país en dos. Se inició una **carrera armamentista** sin precedentes entre la URSS y Estados Unidos capaz de destruir el planeta. Estados Unidos vivió un rápido desarrollo industrial y consumismo masivo. Alemania y **Japón** experimentaron una sorprendente recuperación económica que, menos de dos décadas después del final de la guerra, los había transformado en fuertes potencias económicas, no militares.

su casa de la escuela y pasó la noche solo en una posada, demostrando su independencia y perseverancia. (Valek, 2012).

Turing era muy hábil para lo que realmente le interesaba: resolvía problemas matemáticos avanzados para su edad sin haber estudiado cálculo elemental y cuando sólo contaba con 16 años, comprendió los trabajos del ya entonces reconocido físico Albert Einstein e infirió las críticas de éste a las Leyes de Newton. Sus biógrafos[67] lo describen en esa época como un buen deportista, aficionado al remo y a las carreras, ambicioso y optimista, cuya personalidad cambiaría drásticamente con la muerte de su gran amigo Christopher Morcom, quien falleció de tuberculosis siendo su compañero de colegio.

De 1931 a 1934 Turing estudió en uno de los sitios más prestigiados de Inglaterra, el Kings College de la Universidad de Cambridge, donde se adentró en temas que lo apasionaban como la lógica matemática; en 1935 se graduó con honores y se integró como académico. Un año después viajó a Estados Unidos y, de 1936 a 1938, se incorporó a otro sitio de excelencia académica, el Instituto de Estudios Avanzados de Princeton, donde entraría en contacto con destacados matemáticos, lógicos y físicos como Alonzo Church, Kurt Gödel, Albert Einstein y Max Von Newman, con quien sentaría las bases teóricas de la computación.[68]

En 1936, en el artículo "On Computable Numbers" (sobre los números computables), Turing determinó la naturaleza y limitaciones teóricas de las máquinas lógicas antes de que se construyera siquiera una computadora programable y reformuló los resultados sobre los límites de la demostrabilidad y la computación, obtenidos en 1931 por Gödel. Un año después, en 1937, publicó el célebre artículo en el que definió una máquina calculadora de capacidad infinita –llamada en su honor ***máquina de Turing***– que operaba basándose en una serie

[67] Ya hemos mencionado que entre los principales biógrafos de Turing, a los que hacemos referencia continuamente, se encuentran el ya citado David Leavitt (2006) y los textos y homenajes de Andrew Hodges (1993, 1997 y 2012), así como el sitio http//www.turing.org.uk/ y el artículo sobre Turing de Valek (2012).

[68] Todos ellos (excepto el genial físico teórico, A. Einstein) son pilares de las ciencias de la computación y también hicieron aportaciones fundamentales a las matemáticas y a la lógica.

de instrucciones lógicas y vemos con mayor detalle más adelante y sentó las bases del concepto moderno de ***algoritmo***. Así describió, en términos matemáticos precisos, cómo un sistema automático con reglas extremadamente simples podía efectuar toda clase de operaciones matemáticas expresadas en un lenguaje formal determinado. La máquina de Turing representó, nada más y nada menos, la prueba de que podía construirse una computadora.

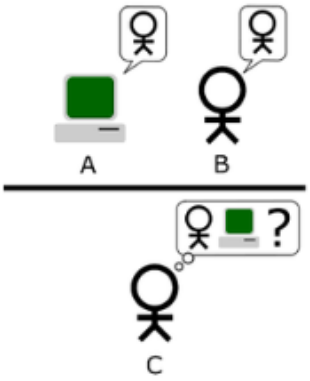
Una ***máquina de Turing*** es un dispositivo que manipula símbolos sobre una tira de cinta de acuerdo a una tabla de reglas, que puede ser adaptada para simular la lógica de cualquier algoritmo de computadora. Originalmente en 1936 fue definida por Turing como una máquina automática. No está diseñada como una tecnología de computación práctica, sino como un dispositivo hipotético que representa una máquina de computación (que ayuda a entender los límites del cálculo mecánico).

Refiriéndose a su publicación de 1936, Turing escribió que la máquina de Turing, (o máquina de computación lógica) consistía en: "... una ilimitada capacidad de memoria obtenida en la forma de una cinta infinita marcada con cuadrados, en cada uno de los cuales podría imprimirse un símbolo. (Turing (1948: 61) [69]

A una máquina de Turing capaz de simular cualquier otra máquina de Turing se la llamó ***máquina universal de Turing*** (UTM, o máquina universal). Una definición más matemáticamente orientada, con una similar naturaleza " universal", la presentó Alonzo Church, cuyo trabajo se entrelazó con el de Turing en una teoría formal de la computación conocida como la tesis de Church-Turing. La tesis señala que las máquinas de Turing capturan, de hecho, la noción informal de un método eficaz en la lógica y las matemáticas y proporcionan una definición precisa de un algoritmo o 'procedimiento mecánico'.

[69] En cualquier momento hay un símbolo en la máquina; llamado el símbolo leído. La máquina puede alterar el símbolo leído y su comportamiento está en parte determinado por ese símbolo, pero los símbolos en otros lugares de la cinta no afectan el comportamiento de la máquina. Sin embargo, la cinta se puede mover hacia adelante y hacia atrás a través de la máquina, siendo esto una de las operaciones elementales de la máquina.

La importancia de la máquina de Turing en la computación radica en que fue uno de los primeros (si no el primero) modelos teóricos para las computadoras y ha sido básica para innumerables desarrollos teóricos en esa área y en la teoría de la complejidad. Cabe aclarar que las máquinas de Turing no son un modelo práctico para la computación en máquinas reales, las cuales precisan modelos más rápidos. La siguiente figura (adaptada de Saygin, 2000) puede esquematizar la prueba de Turing:



La "interpretación estándar" de la prueba de Turing, en la cual la entidad C, el interrogador, le es dada la tarea de tratar de determinar qué entidad (A o B) es una computadora y cuál un ser humano. El interrogador se limita a la utilización de las respuestas a las preguntas escritas para tomar la determinación.

En 1938, en su disertación para obtener el doctorado en Princeton, Estados Unidos, Turing introdujo el concepto de ***hipercomputación***[70] y el estudio de los problemas para los que no existen soluciones algorítmicas. Regresó a Cambridge Inglaterra en 1938 y ante el ambiente bélico fue reclutado por el gobierno británico en la Escuela de Cifrado y Codificación. El 4 de septiembre de 1939, un día después de que el Reino Unido declarara la guerra a Alemania (que ya había invadido varios país de Europa Central)), Turing se trasladó a Bletchley Park, el célebre centro secreto británico de decodificación, ubicado en una vieja mansión

[70] La teoría de la hipercomputación rechaza la idea de una computabilidad absoluta, independiente de cualquier teoría lógica, matemática, física o biológica subyacente. Para implementar un hipercomputador, se requerirían modelos fundamentados en la física y la computación cuántica

en el campo entre Oxford y Cambridge. Ahí el gobierno británico le asignó encargarse de la casona 8, sección responsable del análisis criptográfico de Enigma, máquina usada en mensajes de guerra de la marina germana.

Durante la Segunda Guerra Mundial (1939-1945), aunque hubo muchos científicos de diversas áreas que se abocaron al desciframiento de códigos en ambos lados de los océanos Atlántico y Pacífico, Turing se convirtió en uno de los principales decodificadores de los códigos secretos nazis. Sus atinadas observaciones matemáticas y la concepción y diseño de la *Bomba*[71], así llamada la máquina decodificadora británica, contribuyeron a descifrar la información de la máquina alemana *Enigma* y de los codificadores de teletipos *Fish,* a través de los cuales los nazis transmitían información militar estratégica y secreta.

Entre otras cosas, Turing se basó en el trabajo de criptoanálisis llevado a cabo en Polonia antes de la guerra y específicamente en el realizado por el ingeniero judío Robert Lewinsky, a quien conoció en 1938, que había colaborado con los alemanes en el diseño de un sistema electromecánico de encriptación de comunicaciones y, para fortuna de los aliados, se había pasado del lado británico desde su refugio en Francia.

Mientras la marina alemana empleaba mensajes encriptados para enviar instrucciones a los submarinos que atacaban a los barcos de ayuda material enviados desde Estados Unidos como apoyo a Gran Bretaña, cobrando además miles de vidas, Turing –al frente de un equipo de matemáticos, ingenieros e incluso los mejores jugadores británicos de ajedrez– diseñó tanto los procesos como las máquinas que, capaces de efectuar cálculos combinatorios mucho más rápidamente que cualquier ser humano, fueron decisivos en la decodificación final de los códigos de la marina alemana. Su importancia en la guerra fue crucial pues

[71] La *Bomba* consistía en una máquina electromecánica, mejorada por el matemático Gordon Welchman, que exploraba las combinaciones posibles generadas por *Enigma* y las descifraba. Para cada combinación posible se implementaba eléctricamente una cadena de deducciones lógicas; se podía detectar así cuándo ocurría una contradicción y desechar combinaciones.

gracias a las *bombas,* los británicos pudieron mantener fuera del alcance de los submarinos alemanes muchos de los barcos aliados de suministro con alimentos, armas y diversos materiales que desde Estados Unidos cruzaban el Atlántico hacia Europa.

Los estudios de Turing y de otros matemáticos en Bletchley Park sobre el sistema *Fish,* por su parte, ayudarían también al desarrollo posterior de la que se considera la primera computadora programable electrónica digital llamada *Colossus*. Ésta fue diseñada por el británico Max Newman y su equipo y construida años más tarde, en 1943, en la Estación Británica de Investigaciones Postales de Dollis Hill.

No debe confundirse al matemático británico Max Newman con el matemático estadounidense de origen húngaro John von Neumann. En la mayoría de las historias de la computación se afirma que la primera computadora electrónica de la historia fue ENIAC, desarrollada en la Moore School de la Universidad de Pensilvania, al final de la Segunda Guerra Mundial, y que la primera computadora con programa almacenado fue EDVAC, desarrollada poco después. Debido a que su diseño se debió al matemático John von Neumann, se habla de una arquitectura "tipo von Neumann" para referirse a una computadora convencional que ejecuta sus instrucciones de forma secuencial y que almacena su programa en la misma memoria que los datos. Aunque profundizamos en este aspecto en los siguientes apartados, vale mencionar aquí que a Turing se le reconocen sus contribuciones en la concepción y nacimiento práctico de las computadoras electrónicas.

La primera *Bomba* de Turing se instaló el 18 de marzo de 1940; al final de la guerra había en operación más de 200. Su construcción y los trabajos de decodificación de Turing y sus colegas de Bletchley Park se mantuvieron en estricto secreto hasta los años setentas del siglo XX; nunca los compartieron siquiera con sus amigos más íntimos y el gobierno británico los guardaba

celosamente. Así, la vida de Turing transcurrió entre guerras, secretos personales y profesionales, algunos importantes logros y fuertes desilusiones.

No abundaremos sobre la homosexualidad de Turing aunque fue un factor importante para delinear su excéntrica personalidad y aislamiento. Estuvo siempre dedicado al trabajo, excepto por un corto periodo, en 1941, cuando contempló la idea de casarse e incluso propuso matrimonio a Joan Clarke, una colega matemática de Betchley Park, quien rompió el compromiso al enterarse de su homosexualidad, cada vez más explícita y evidente en una época en que no sólo era mal vista sino que estaba prohibida.

En julio de 1942, completamente dedicado a sus investigaciones, Turing desarrolló una técnica de cifrado y descifrado a la que llamó primero Turingery (o Turingismus) y acabó siendo implementé conocida como Tunny, para contrarrestar los mensajes cifrados alemanes. Ese año viajó nuevamente a Estados Unidos y trabajó con criptoanalistas navales americanos en Washington y en los importantes Laboratorios Bell en el desarrollo de dispositivos discursivos seguros y de SIGSALY, un sistema que sería usado en los últimos años de la guerra.

Como veremos más adelante, los Laboratorios Bells serán determinantes en el trabajo informático y criptográfico sobre todo de Shannon. Se originan en 1925, como *Laboratorios Telefónicos Bell*, fundados por la empresa AT&T y luego parte de Lucent Technologies. Entre sus patentes más importantes destacan el transistor, el láser, la fibra óptica, la tecnología DSL, la telefonía móvil, los satélites de comunicaciones, el sistema operativo Unix, lenguajes de programación. Once de sus investigadores han obtenido Premios Nobel. Ahí Turing conoció a Shannon y como veremos más adelante en el capítulo VI de este trabajo, aunque coincidieron algunos días en ese lugar, al parecer no compartieron ni sus conocimientos ni sus secretos.

Turing regresó a Bletchley Park en 1943 como asesor en criptoanálisis y, poco después, se mudó a trabajar a Hanslope Park donde, con el ingeniero Donald Bayley, diseñó y construyó una máquina de comunicación llamada *Dalilah* para las transmisiones de radio de larga distancia, que no alcanzaría a usarse en la guerra.

Pocos meses después, en 1945, el matemático Max Newman fue nombrado jefe de la Escuela de Matemáticas de la Universidad de Mánchester, donde fundó el Royal Society Computing Machine Laboratory y reclutó a matemáticos e ingenieros y, con Thomas Kilburn, construyó la primera computadora de la historia con programas informáticos almacenados de forma electrónica, basadas en las ideas de Turing.

Terminada la guerra y con acelerados avances tanto en desciframiento de códigos como en computación, de 1945 a 1948 Turing trabajó en el Laboratorio Nacional de Física de Gran Bretaña en el diseño de un motor de computación automática, ACE, por sus siglas en inglés. En 1946 había presentado el primer diseño detallado de un programa de almacenamiento de cómputo. Aunque era un proyecto aplicable, el secreto alrededor del trabajo de guerra generó retrasos y Turing, desilusionado, regresó a Cambridge, en 1947, en un año sabático. Mientras tanto, en su ausencia se construyó el piloto ACE, que ejecutaría su primer programa en mayo de 1950.

También por esa época, en 1948, Turing inventó un método para resolver ecuaciones, usado hoy en matemáticas, y empezó a escribir un programa de ajedrez para computadora que incluso llegó a *jugar* con una persona.[72] Conoció a

[72] Décadas más tarde, *Deep Blue* fue una supercomputadora desarrollada por el fabricante estadounidense IBM para jugar al ajedrez. Fue la primera que venció a un campeón del mundo vigente, Gary Kaspárov, con un ritmo de juego lento. Esto ocurrió el 10 de febrero de 1996, en una memorable partida. Véase *Deep Blue*. IBM Research. Consultado el 23 de abril de 2011 y "Garry Kasparov vs Deep Blue", 12 games. Chessgames.com. Consultado el 23 de abril de 2011.

Norbert Wiener[73] quien introdujo y desarrolló la cibernética, entre cuyos objetivos se encontraba establecer un sistema de comunicación entre el hombre y la máquina para administrar sistemas de control. Sus estudios profundizaron en esa relación estableciendo el concepto de ***interfaz*** y cuestionando los límites de la simulación del razonamiento humano.

En 1949 Turing fue nombrado director delegado del Laboratorio de Computación de la Universidad de Manchester y trabajó en la programación de una de las primeras computadoras y en el programa MADAM (Manchester Authomatic Digital Machine) que resultó ser el equipo de computación de mayor memoria construido hasta entonces.

En 1950 se publicó *Computing Machinery and Intelligence* donde en 1950 Turing expresó su convicción de que es posible simular la inteligencia humana con la computadora. Al prometer *o amenazar* sustituir al hombre, la computadora –escribió– ofrece una nueva definición de hombre, como *procesador de información*, y de la naturaleza, como *información que debe ser procesada*. Para definir si una máquina puede catalogarse como *inteligente*, propuso la prueba conocida ahora como Prueba o ***Test de Turing*****,** que se basa en la idea siguiente: si una persona se comunica a través de una terminal con otras dos partes, que están escondidas y no se puede discriminar a través de preguntas cuáles la persona y cuál el ordenador, entonces no se puede negar que la máquina muestra la cualidad que, en las personas, se llama inteligencia. Turing creía firmemente que máquinas que simulan el pensamiento llegarían a existir hacia el año 2000. Estas aportaciones con respecto a la inteligencia artificial fueron el centro de debates por más de medio siglo. (Valek, 2012).

[73] Este matemático estadounidense (Columbia, Mi., Estados Unidos, 1894-Estocolmo, Suecia, 1964) fundador de la cibernética, acuñó el término en su libro *Cibernética o el control y comunicación en animales y máquinas*, publicado en 1948.

Pocos años antes de morir, Turing se dedicó al estudio de la biología matemática y escribió "Fundamentos químicos de la morfogénesis",[74] que aporta luz sobre la existencia de los ***números de Fibonacci*** en las estructuras vegetales y utilizó ecuaciones de reacción-difusión, hoy cruciales para la formación de patrones.[75]

Sus biógrafos[76] muestran a Turing como un hombre fuerte, robusto y parlanchín, conocido por su enigmática personalidad, al que le gustaba tocar el violín, aunque no lo hacía muy bien. Cada año, al inicio de la primavera, sufría de ataques de fiebre del heno por lo que llegaba a trabajar portando una máscara de gas para protegerse del polen. La cadena de su bicicleta –medio de transporte de los académicos en Cambridge y en Bletchley Park– se zafaba y, en lugar de arreglarla, contaba el número de veces que los pedales daban la vuelta y se bajaba a tiempo para ajustar la cadena. Se le recuerda también atando su taza de té al radiador para evitar que se la robaran; corriendo los 64 km de distancia de Bletchley Park a Londres para asistir a alguna reunión, y la tristeza que le produjo una lesión en la cadera que le impidió competir en los Juegos Olímpicos, uno de sus sueños.

La vida de Turing cambió drásticamente cuando en 1952 su amante y un cómplice entraron a robar a su casa. Al denunciarlos, Turing debió reconocer públicamente su homosexualidad y se le imputaron los cargos de *indecencia grave y perversión sexual*. Después del juicio fue condenado y se le dio a escoger entre ir a prisión o someterse a un tratamiento hormonal. Turing prefirió este último por lo que se le aplicaron inyecciones de estrógenos durante un año, ocasionándoles serias alteraciones físicas y emocionales (Valek, 2012).

[74] Según explica Reinitz, John (2012) Turing formuló un modelo clave para entender la formación de patrones en los seres vivos. El artículo de 1952 en el que Turing expuso su teoría sobre la formación de patrones en sistemas biológicos resolvió un profundo problema intelectual.

[75] Para capturar las reglas elementales de la acción mecánica (o máquina de Turing), "La esencia de la programación (es decir del arte de capturar las reglas básicas de la acción) es la de describir los pasos de un proceso cualquiera en sus unidades mínimas, uno a uno, en forma unívoca. En el modelo prototípico de Turing, las acciones se especifican unívocamente, "movimiento de células a la derecha/izquierda, Imprimir/borrar, cambiar de estado interno" Flores Morador, (2003).

[76] Entre los que por supuesto se encuentran los ya citados Hodges (1983, 1987 y 2012) y Leavitt (2006), además de Agar Jon *(2001)* y Teuscher, C. (2004).

Dos años después del proceso que afectó seriamente su vida profesional y su salud, el 8 de junio de 1954 una persona de servicio halló a Turing muerto en su casa de Cheshire. El examen *post mortem* estableció que había fallecido un día antes por envenenamiento con cianuro, que se encontró en los restos de una manzana al lado de su cama. Días después de que terminó la escandalosa investigación policial –que llegó a contemplar desde muerte accidental por químicos de su laboratorio hasta el suicidio e incluso el asesinato– su cuerpo fue cremado.

En vida, aunque se le confirió la Orden del Imperio Británico y se le invitó a formar parte de la prestigiosa Royal Society, no se le dio el reconocimiento merecido. Hoy, a más de un siglo de su nacimiento, en varios institutos y universidades del mundo (y por supuesto en Cambridge, Bletchley Park y Manchester) hay estatuas que conmemoran su impresionante trayectoria. La *Association for Computing Machinery* otorga anualmente el Premio Turing, considerado el equivalente del Premio Nobel en el mundo de la computación y en el verano de 2004 se inauguró en la Universidad de Manchester el Instituto Alan Turing.

Su rostro ilustra estampillas y sellos postales y da nombre a puentes, plazas, laboratorios, jardines, calles y avenidas en Inglaterra y Estados Unidos como el padre de las ciencias de la computación y de la inteligencia artificial, aunque ese término se usara hasta 1956. El *Turing Centenary Advisory Committee* y asociaciones europeas, en colaboración con académicos británicos, entre los que se encuentra su sobrino, Sir John Dermot Turing, organizaron durante el año 2012 un amplio programa de conferencias en Manchester y Cambridge sobre sus aportaciones en el campo de las matemáticas, la lógica y la de codificación de mensajes. Nadie fue invitado de las ciencias sociales y mucho menos de las ciencias de la comunicación, aspecto en el que profundizamos más adelante.

Turing es un personaje protagónico en varias obras literarias; en 1999, *Time Magazine* lo nombró uno de los *100 Personajes Clave del Siglo XX* porque "… cada persona que tecleé en una computadora o abra un programa está trabajando en la encarnación de la máquina de Turing" y, en 2002, fue catalogado por la BBC el número 21 dentro de los *100 Grandes Británicos* y, agregaríamos, del mundo. Su vida fue fructífera e intensa y resulta curioso (y apenas justo) que la movilización pública para limpiar su nombre haya tomado fuerza sobre todo a través de las redes sociales digitales, que deben a Turing gran parte de su existencia. (Valek, 2012).

En palabras de Eric Hobsbawm: "…el célebre texto de Alan Turing de 1935, que proporcionaría los fundamentos de la moderna teoría informática, había sido escrito originalmente como una exploración especulativa para lógicos matemáticos. La guerra dio a él y a otros científicos la oportunidad de traducir la teoría a unos primeros pasos de la práctica empleándola para descifrar códigos, pero cuando el texto se publicó originalmente, nadie, a excepción de un puñado de matemáticos, pareció enterarse de sus implicaciones. Este genio de tez pálida y aspecto desmañado, que era por aquel entonces un joven becario aficionado al *jogging* y que se convirtió póstumamente en una especie de ídolo para los homosexuales, no era un a figura destacada ni siquiera en su propia facultad universitaria, o al menos yo no lo recuerdo como tal. […] Turing no pudo soportar la «cura» que le impusieron. No fue tanto una víctima de la criminalización de la homosexualidad (masculina) en Gran Bretaña antes de los años sesenta, como de su propia incapacidad para asumirla. Sus inclinaciones sexuales no provocaron ningún problema en el King's College de Cambridge, ni entre el notable conjunto de personas raras y excéntricas que durante la guerra se dedicaron a descifrar códigos en Bletchley…". [77]

[77] Como vimos en las biografías y en el artículo de G. Valek citado anteriormente, Turing se suicidó en 1954, tras haber sido condenado por comportamiento homosexual, que por aquel entonces se consideraba un delito y también una patología que podía curarse mediante un tratamiento médico (*terapia hormonal*) o psicológico. (Hobsbawm, 1994: 221).

En aquel entonces, recuerda Hobsbawm que incluso como "…becario en Cambridge durante la misma época en que Crick y Watson preparaban su triunfal descubrimiento de la estructura del ADN (la «doble hélice»), que fue inmediatamente reconocido como uno de los grandes acontecimientos científicos del siglo… la mayoría de nosotros ignorábamos por completo que tan extraordinarios acontecimientos tenían lugar a pocos metros de la puerta de nuestra facultad, en laboratorios ante los que pasábamos regularmente y en bares donde íbamos a tomar una copas […] las innovaciones científicas, una vez logradas, se traducían casi inmediatamente en tecnologías prácticas. Así, se crearon los transistores y hubo muchos otros inventores que también obtuvieron el premio Nobel; se investigaba sobre la física de bajas temperaturas (luego, los superconductores).

Las investigaciones realizadas durante la guerra, entre 1939 y 1946, demostraron a los anglosajones que la gran concentración de recursos podía resolver los complejos problemas tecnológicos en poco tiempo; eso animó a una búsqueda tecnológica con fines bélicos o por prestigio nacional, como en la posterior exploración del espacio. Esto aceleró la transformación de la ciencia básica (teórica) en tecnología para la industria y la vida cotidiana; una tecnología que no requería ningún tipo de comprensión por parte de los usuarios finales.[78]. Con esta maravillosa descripción nos quedamos por ahora.

II.5. Claude E. Shannon, creador innato

Petoskey, la pequeña localidad en la que nació Shannon hace poco más de cien años, era apacible y pintoresca. Su padre era juez y notario, gran amante de las matemáticas, y su madre profesora de enseñanza media. La infancia y juventud de Shannon transcurrieron sin grandes sobresaltos pero fueron decisivos pues uno de sus abuelos era un inventor ocioso que, además, reparaba con

[78] Para Hobsbawm (1994, 220-222) "Ha quedado claro que si la Alemania nazi no pudo hacer la bomba atómica, no fue porque los científicos alemanes no supieran cómo hacerla… sino porque la maquinaria de guerra alemana era incapaz de dedicar a ello los recursos necesarios. Abandonaron por ello el esfuerzo y se concentraron en lo que les pareció más efectivo: los cohetes, que prometían más beneficios…",

entusiasmo máquinas y objetos. De hecho, el abuelo poseyó la patente de una lavadora y creó diversos aparatos y utensilios a veces inútiles pero llenos de inventiva y espíritu creativo. Con estos ejemplos en casa, el joven Shannon se volvió un creador en potencia y un ferviente admirador de los grandes inventores de la época, entre los cuales su preferido era el reconocido Thomas Alva Edison con quien, como descubriría años más tarde, estaba lejanamente emparentado. (Valek, 2016).

Al terminar la enseñanza secundaria y en tiempos de paz, el joven Shannon ya había construido diversos juguetes y algunos aparatos, entre ellos un pequeño barco teledirigido y un sistema telegráfico basado en alambres con el que se comunicaba con sus amigos a varios metros de distancia. En su tiempo libre seguía también los pasos de su abuelo pues arreglaba radios y otros aparatos por módicas cantidades de dinero. Su trayectoria científica comenzó con el estudio del ***álgebra booleana***, rama de las matemáticas que George Boole desarrolló para describir las propiedades básicas de las operaciones lógicas y que Shannon aplicaría años más tarde en el diseño de circuitos de conmutación eléctrica.

A lo largo de su vida, Shannon estuvo vinculado a importantes centros de investigación como el Instituto Tecnológico de Massachusetts (MIT por sus siglas en inglés), el Instituto de Estudios Avanzados de Princeton y los reconocidos Laboratorios Bell y estuvo muy cerca de científicos destacados en computación, matemáticas, comunicaciones y tecnología como Vannevar Bush, Hermann Weyl, John von Neumann[79]. Norbert Wiener y el propio Alan Turing.

Shannon se graduó en ingeniería eléctrica y matemáticas en la Universidad de Michigan y empezó a trabajar en el Departamento de Ingeniería Eléctrica del MIT, donde encontró una manera de combinar sus pasiones y capacidades mientras seguía estudiando: reparaba objetos y aplicaba sus conocimientos en ingeniería

[79] Vannevar Bush, Hermann Weyl y John von Neumann hicieron importantes aportaciones a las ciencias de la computación tanto para el software como para el desarrollo posterior de programas informáticos específicos y, en algunos casos, incluso, trabajaron paralelamente a los intereses de Turing y Shannon.

eléctrica al mantenimiento de máquinas, entre ellas las primeras calculadoras para resolver ec uaciones y c álculos, y en es pecial un an alizador diferencial (computadora analógica mecánica di señada par a s olucionar ecuaciones diferenciales). Este úl timo fue c onstruido p or Vannevar B ush –quien s ería s u maestro, ejemplo y mentor durante los siguientes años– y fue uno de los primeros dispositivos de computación avanzados en ser usados operacionalmente. Bajo su supervisión, Shannon escribiría en 19 37 su tesis de maestría, sobre interruptores controlados p or c ircuitos eléctricos, l lamados ***relevadores*** y de c ircuitos de conmutación o conjuntos de interruptores que permiten o impiden la circulación de una c orriente el éctrica. E n u na en trevista r ealizada añ os d espués y q ue reproducen sus colegas, Shannon recordó: "…el álgebra booleana era justo lo que hacía falta para ocuparse de los circuitos de relés y de conmutación. Me dirigí a la biblioteca y r euní t odos l os l ibros q ue p ude s obre l ógica s imbólica y ***álgebra booleana*** empezando la interconexión entre ambos y escribí mi tesis de maestría sobre esto. ¡Ese fue el principio de mi gran carrera!". (Valek, 2016).

Décadas m ás tarde, H. Goldstine (1972)[80], en s u l ibro *Las computadoras desde Pascal hasta Von Neumann* explicó q ue l a t esis de S hannon ay udaría a transformar el ar te d el di seño de c ircuitos en un a c iencia, pu es des arrolló u n método riguroso de análisis y síntesis de los circuitos, demostrando cómo podían simplificarse. Entre o tras c osas, S hannon s e c entró en l as r elaciones en tre propiedades c omo l a redundancia y el l ímite de e ficiencia, fundamentales par a transmitir i nformación en l a t elefonía, l a r adio, l a t elevisión, l a t elegrafía, et c. (Valek, 2016).

Entre 1939 y 19 45 m uchas i nstituciones pú blicas, e mpresas y un iversidades de Estados Unidos comenzaron a s umarse al esfuerzo bélico de l a Segunda Guerra Mundial. En ese país se fundaron varios centros, organizaciones y oficinas como el C omité de I nvestigación par a l a D efensa N acional, b ajo l a s upervisión d e

[80] Herman Heine Goldstine (1913–2004), matemático, informático y administrador científico fue uno de los principales desarrolladores de ENIAC, el que se dice fue el primer computador electrónico digital de propósito general.

Vannevar Bush, y la Oficina de Investigación Científica y Desarrollo, dedicadas ambas casi totalmente a la nueva guerra.

Mientras tanto, Shannon había continuado su trabajo sobre el uso del álgebra y comenzó sus estudios de doctorado con el matemático Frank L. Hitchcock. A sugerencia de Bush, Shannon aplicó el ***álgebra booleana*** a la genética como lo había hecho a los circuitos y meses después de haber estallado la Segunda Guerra Mundial, presentó su tesis "Un algebra para la genética teórica". También en 1940 comenzó a trabajar en los Laboratorios Bell y se le otorgó el premio Alfred Nobel de la Sociedad Estadounidense de Ingeniería Civil por la tesis de maestría en la que ilustró sus planteamientos.

Poco después, en 1941, Shannon publicó su "Teoría matemática del analizador diferencial" y durante algunos meses trabajó bajo la supervisión del reconocido matemático alemán Hermann Weyl en el Instituto de Estudios Avanzados de Princeton, gracias a una beca nacional de investigación. Poco después se reintegró a los Laboratorios Bell, una institución fructífera y de gran prestigio, con destacados matemáticos y científicos como el ingeniero eléctrico John Pierce, conocido por sus aportaciones a los satélites de comunicaciones, Harry Nyquist, famoso por sus contribuciones a la teoría de señales, y Brattain, Bardeen y Shockley, inventores del transistor. Ahí trabajaría Shannon durante toda la guerra y hasta 1956. (Neil J. Sloane y Aaron D. Wyner eds., 1993).

Como otros científicos, matemáticos e ingenieros, Shannon participó en la investigación bélica, principalmente en dos proyectos: el primero sobre artillería antiaérea, esencial para el contraataque de Gran Bretaña, principal aliado de Estados Unidos, y en la defensa contra los misiles alemanes V1 y V2, que tanto daño hacían a las poblaciones inglesas. Shannon trabajó específicamente en los parámetros de control de disparo que debían determinarse automáticamente a partir de los datos del radar y con otros ingenieros y matemáticos de los Laboratorios Bell desarrolló sistemas de control de fuego (como transmisión y

manipulación) y de procesamiento de señales. Mantuvo también contacto con Warren Weaver, director de la División de Ciencias Naturales de la Fundación Rockefeller quien, como ya mencionamos, revisaría y enriquecería su famoso artículo sobre la teoría matemática de la información y se convertiría en su coautor (Valek, 2016).

El segundo proyecto bélico en el que se centró Shannon se relacionó con la criptografía, un campo estratégico durante la guerra pues las comunicaciones podían interceptarse fácilmente. El principal medio de comunicación trasatlántico para mensajes confidenciales era el sistema telefónico A3, desarrollado en los Laboratorios Bell, que sólo invertía partes del ancho de banda y que por su simplicidad era fácilmente descifrado por los alemanes. Shannon trabajó en el sistema X, que resolvía ese problema y durante ese periodo se encontró con Alan Turing, quien había llegado a los Laboratorios Bell para coordinar la investigación británica y estadounidense sobre interferencia. (Valek, 2016). Sin embargo, su encuentro no fue muy fructífero pues aunque ambos trabajaban en temas afines, las prioridades de cada uno eran los secretos de guerra de sus respectivos países.[81]

La principal contribución de Shannon a la criptografía bélica se encuentra en el informe de 1945, desclasificado en 1957, titulado "Teoría matemática de la criptografía", que se apoya en la probabilidad y los conjuntos numerables (aquellos que se pueden poner en correspondencia con el conjunto de los números naturales) para desarrollar códigos y formas más seguras de encriptar. Definió ahí los términos *redundancia, equivocidad, información* y *entropía,* como llamó a la función de *incertidumbre*, y desarrolló un esquema para una comunicación segura pero siempre pensando en su teoría de la información.

[81] Algunos de sus biógrafos como Tsybakov, Boris, (Recuperado en http://echo.gmu.edu/shannon/survey/memories.php) se refieren a su encuentro como algo casual; otros, a cierta afinidad pero los más a la ignorancia mutua uno del otro. Abundaremos en su encuentro en los siguientes capítulos.

Basándose en su experiencia en los Laboratorios Bell, donde había trabajado con otros ingenieros de telecomunicación, Shannon publicó en 1948 en dos números del *Bell System Technical Journal* su artículo "Teoría matemática de la comunicación". En términos simples, ésta define la cantidad de información que contiene un mensaje, con base en las probabilidades con las que pueden darse los símbolos que lo componen. Su enfoque era puramente pragmático pues quería estudiar "los ahorros debidos a la estructura estadística del mensaje original" y, para ello, dejó de lado los aspectos semánticos de la información pues, como ya mencionamos, no explicó lo referente al contenido del mensaje, ni le interesaba hacerlo.

En su artículo "Teoremas fundamentales", Shannon asentó que haciendo una buena elección del transmisor y del receptor es posible enviar información de manera exacta y confiable, siempre y cuando el ritmo de transmisión de la información no exceda un límite fundamental o *capacidad de canal*. El artículo presenta un conjunto de 23 ***teoremas*** y se divide en cuatro partes que distinguen entre distintas fuentes y abordan la presencia o ausencia de ruido. En el caso del teorema más sencillo (el de *fuentes discretas sin ruido*), Shannon presenta la denominada *fórmula H* (donde H equivale a información y que ya había definido en su teoría matemática de la criptografía).

Shannon definía el *bit*, contracción de *binary digit* (bajo sugerencia de John W. Turkey, colega de los Laboratorios Bell), como la unidad de información y el elemento fundamental de la comunicación. Shannon acuña allí este término y define nociones ya existentes como *redundancia*, *equivocidad*, o *capacidad* de canal desde el punto de vista científico, mostrando que *la longitud promedio de un mensaje tiene un límite mínimo proporcional a la entropía o grado de organización de la fuente*. Al introducir ruido, el *teorema de codificación* de canal establece que cuando la entropía de la fuente es menor que la capacidad del canal, existe un código que permite transmitir un mensaje "de modo que la salida de la fuente puede transmitirse a través del canal con una frecuencia de errores

arbitrariamente baja". Es decir, para que el cifrado sea lo más perfecto posible, cuando se usa el mismo alfabeto o conjunto de símbolos para la llave (o clave) y para el mensaje, la longitud de la llave debe ser mayor o igual a la longitud del mensaje. (Valek, 2016).

El artículo de 1948 se hizo rápidamente famoso y se publicó poco después como libro, con el texto de Warren Weaver (1949), quien agregó algunos aspectos semánticos de la información, que no tardaron en interesar y ser criticados por estudiosos de las ciencias sociales y de la naciente disciplina de la comunicación, urgidos estos últimos por definir y diferenciar los procesos y fenómenos de la información y la comunicación.[82]

Los años posteriores a la publicación de las teorías de la información y la criptografía de Shannon, los ingenieros reconocieron el valor programático de sus escritos y los matemáticos, el desarrollo de nuevas técnicas de codificación y la definición matemática de información, que para Shannon significaba entropía (por analogía al definir dicha magnitud en la termodinámica) e indica el grado de orden de un sistema. Estas ideas se fundieron con otras aportaciones de la posguerra como la de una teoría general para el "Control y comunicación en animales y máquinas", subtítulo de *Cybernetics*[83]*,* el libro que Norbert Wiener publicó en 1948 y que, con la obra de Shannon y Weaver, impulsó el nacimiento de la denominada *era de la información*.[84]

Desde el ***álgebra booleana***, Shannon teorizó acerca del código binario, la base del lenguaje digital, a partir de unidades básicas de información, definidas por dos estados: el 'sí' y el 'no', el 0 y el 1, abierto/cerrado, verdadero/falso, blanco/negro. Estableció que el 0 y el 1 son la base de la información, la base constructiva del mensaje; una información compleja es una sucesión de unidades básicas, de unos

[82] Entre los textos clásicos de las ciencias de la comunicación y los debates teóricos sobre la diferenciación entre información y comunicación, véase Mattelart, A. (1999) y recientemente Karam, Tanius (s.f.) y sus gráficas sobre los principales teóricos y corrientes de estudio de la comunicación.
[83] Sobre este tema, véase Valek, G. (2010) y Rosenblueth, Arturo (1970)
[84] Véase la excelente obra de Castells Manuel *(*1996).

y c eros. Más al lá de l a f ormulación t eórica, c onstruyó c ircuitos y m áquinas basadas en los flujos binarios de información, mediante interruptores y relés[85] en los que se anticipaban muchos de los desarrollos de las siguientes décadas. La información tratada así adquirió una dimensión física, cuantificable y mesurable, independientemente del contenido, de los emisores y los receptores.

Shannon er a una p ersona obsesiva p ero t ambién di vertida; par a pr obar empíricamente sus ideas, viajó varias veces a Las Vegas con su esposa, pues uno de sus colegas en los Laboratorios Bell había demostrado cómo podía aplicarse la teoría de la información a los juegos de azar; incluso inventó una máquina portátil capaz de c alcular l os r esultados d e una r uleta. S iempre fue un c onstructor entusiasta de artefactos; se divertía creando prototipos como una calculadora de números romanos, un *frisbee* impulsado por un cohete, un dispositivo que permitía resolver el *cubo de Rubik*, una taza de baño (WC) automática, juegos electrónicos de ajedrez, instrumentos musicales, juguetes mecánicos y relojes. Ideó muchos autómatas q ue g uardaba c on or gullo en s u c asa, e ntre l os q ue des tacaba un pequeño escenario sobre el que tres payasos hacían malabares con once anillos, siete b olas y c inco m azos, t odos i mpulsados por u n mecanismo de r elojería y varillas. Le g ustaba j ugar aj edrez, m ontar su m onociclo particularmente por las noches y tocar el clarinete. (Valek, 2016).

Shannon d emostró q ue en una c omunicación c on p erturbaciones, la s eñal s e puede transmitir s in distorsión s i el mensaje s e c odifica c on un ***sistema de autocorrección***. S u t rabajo per mitió d efinir l a **información** en t érminos matemática y oper acionalmente pr ecisos, medir s u c antidad *(bits)* en di versos sectores y di sciplinas, as í c omo m ejorar l as t écnicas par a s u t ransmisión y tratamiento. C onvirtió l a i nformación e n un a ent idad c oncreta y gener al; e n un a

[85] Un **relé** o **relevador** (inventado por Joseph Henry en 1835) es un dispositivo electromagnético que funciona como un interruptor controlado por un circuito eléctrico en el que, por medio de una bobina y un electroimán, se acciona uno o varios contactos que permiten abrir o cerrar otros circuitos eléctricos independientes. Dado que puede controlar un circuito de salida de mayor potencia que el de entrada, se considera como un amplificador eléctrico. Así se emplearon en telegrafía como repetidores que generaban una nueva señal con corriente procedente de pilas locales a partir de la señal débil recibida por la línea.

mercancía universal tratable de manera industrial; ayudó, como precisaremos más adelante, al desarrollo de las actuales TIC.

Los bi ógrafos de S hannon[86] coinciden en que c on su c oncepto de ***entropía*** estableció un a conexión i ntelectual, a par tir de noc iones matemáticas y probabilísticas, ent re l as i deas de or ganización de l os s istemas f ísicos y l a cantidad de i nformación. C on e sta t eoría s entó l as b ases c onceptuales y matemáticas para el desarrollo de *la sociedad de la información industrializada* en la segunda mitad del siglo XX.

Claude Elwood S hannon m urió en f ebrero de 2001 a los 84 años de eda d, después de sufrir durante décadas la enfermedad de Alzheimer. A lo largo de su vida recibió condecoraciones y reconocimientos de universidades y otros centros académicos d el mundo. F ue m iembro d e l as i nstituciones c ientíficas más importantes de s u pa ís, de l a R oyal S ociety br itánica y de varias s ociedades japonesas. E n 197 2 s e i nstituyó el Premio C laude E . S hannon del Instituto d e Ingeniería Eléctrica y Electrónica (IEEE, por sus siglas en inglés) para reconocer la investigación en el campo de la teoría de l a información y desde entonces se ha otorgado cada año a los académicos más destacados en esa área.

Varias de l as instituciones que lo formaron, como la Universidad de Michigan, el MIT y los Laboratorios Bell se unieron para promover la emisión de un sello postal conmemorativo del centenario de Shannon por considerarlo "el mayor símbolo de la innovación estadounidense" y por "su impacto sin paralelo en la tecnología que marca nuestras vidas". *(*Valek, 2016).

II. 6. Flujos de información entre dos

Cuando el matemático británico Alan M. Turing escribió el primer programa para jugar al aj edrez de f orma au tomática, del ot ro l ado del A tlántico, el i ngeniero estadounidense C laude E . S hannon a portó al gunas s ugerencias t eóricas s obre

[86]Entre los que destaca Tsybakov, Boris, (s.f.) y su texto "Remembering Claude Shannon".

cómo hacerlo con programas adaptados y desarrolló un ratón mecánico con capacidad de *aprendizaje* en laberintos (Valek, 2016).

Según consta en documentos compilados por Sloane, Neil J. y Aaron D. Wyner eds. (1993), en su artículo de 1950, titulado "Programación de una computadora para jugar ajedrez", Shannon ofreció los elementos clave para escribir un ***programa*****,** como una *función de evaluación* o un *procedimiento* ***mini-max*** (un tipo de algoritmo de búsqueda que ayuda a decidir cómo minimizar la pérdida máxima cuando jugamos contra alguien más).

Tal y como lo hemos asentamos en este apartado, tanto Turing como Shannon, crearon herramientas indispensables para el futuro desarrollo de la computación y de las TIC, aspectos en los que profundizamos en los capítulos III, IV y V de este trabajo.

Capítulo III
Principales modelos y escuelas de comunicación

Después de la ubicación espacio-temporal en los apartados descriptivos que han precedido esta investigación y que nos han permitido entender el momento y las circunstancias que vivieron Turing y Shannon, en este capítulo retomamos las principales teorías y acercamientos al estudio de las ciencias de la comunicación que podrían relacionarse con la criptografía computacional y ponemos de manifiesto que pese a la trascendencia de ambos en la comunicación en general y en las TIC en particular, han sido ignoradas sus aportaciones a su desarrollo. Con el fin de aterrizar nuestro bagaje teórico y poder interpretar, reinterpretar y enriquecer nuestros objetos de estudio, exploramos someramente las principales escuelas y teorías de la comunicación que podrían haber tomado en cuenta a la criptografía computacional..

Por ahora partimos del proceso comunicativo con la definición más básica: como la transferencia de información de un emisor a un receptor, asegurándose el primero que la información sea comprendida por el segundo. El proceso de comunicación se inicia con un emisor, quién tiene algo que comunicar. Cuando es necesario, la información se transmite a través de un canal que vincula al emisor con el receptor. El mensaje puede ser verbal, visual o escrito y debe transmitirse a través de una carta, un correo electrónico, el teléfono, un telegrama o a través de medios audiovisuales de comunicación. El receptor recibe el mensaje y, para poder comprenderlo, lo decodifica. Tanto el emisor como el receptor deben tener los mismos códigos. El proceso de la comunicación ocurre cuando el mensaje sea comprendido. Con el objetivo de verificar la comprensión del mensaje enviado, se requiere de la retroalimentación. La comunicación, de esta forma, se realiza en forma invertida ya que el receptor se convierte en emisor y el emisor, en receptor.

Por razones prácticas y dado que no cuestionamos y sólo describimos algunas de las principales teorías de la comunicación, partimos de las divisiones de Tanius Karam (2005) y sus apreciaciones teóricas del análisis de la comunicación a partir de un reconocido investigador de nuestra área de estudio, el catedrático español Manuel Martín Serrano.[87] Todo esto lo hacemos sin olvidar la herramienta fundamental de este trabajo, la hermenéutica profunda y nuestras principales categorías de análisis: el tiempo, el espacio y el desarrollo tecnológico, específicamente con respecto a las ciencias de la comunicación y a las TIC durante los primeros sesenta años del siglo XX y su vínculo con la comunicación secreta y con la criptografía computacional.

Comencemos pues con una revisión general sobre las principales teorías y modelos de comunicación y cómo éstos han ignorado o incomprendido a dos de los autores que han hecho trascendentes aportes no sólo a nuestro campo de estudio sino también a la forma de comunicación actual.

III.1. La comunicación y sus modelos

Hay varios textos que son representativos de las principales escuelas y teorías de la comunicación a los que iremos refiriéndonos en este apartado[88] pero para los fines de esta investigación partimos –con Karam– de la obra de Martín Serrano pues ésta "…sirve para presentar una nueva caracterización de la teoría y epistemología de la comunicación así como la fundamentación para una ciencia de la comunicación". Para ello, parte atinadamente de "las primeras preguntas que ofrece sobre el encuentro epistemológico de las ciencias a través de la comunicación, algunos rasgos de su teoría de la comunicación y su teoría social,

[87] Véase Karam, T. (2005: 253-264) y las obras originales de Martín Serrano, Manuel (1977, 1978, 1982, 1993) y Martín-Serrano *et al. (*1982). Coincidimos con Karam (2005, 15) en que "Martín Serrano es uno de los autores que en castellano más se ha preocupado de fundamentar la sustancia científica de la comunicación mediante el análisis de sus nexos básicos con la física, en el estudio de los cambios de energía y sus soportes de información; la biología, en el estudio de los órganos biológicos que sirvan para modelar la energía y captarla; la etología, en el estudio de los patrones expresivos de la conducta y sus matrices; las ciencias económicas, en el estudio de objetos y bienes, a través de sus asociaciones y representaciones determinante; la psicología y la psiquiatría, en el estudio de los comportamientos considerados normales y anormales".

[88] Véase los textos de Ferrer, Eulalio (2001), Fuentes Navarro, Raúl (2004) y Martín Serrano(1977 y 1993).

así como la descripción de los modelos que estudian los fenómenos de comunicación". (Karam, 2005: 15). Tomemos pues este análisis como punto de partida en este capítulo que, insistimos, no pretende cuestionar las bases teóricas o epistemológicas de esas teorías sino describirlas y, con ello, hacer patente la omisión de la que han sido objeto tanto Alan M. Turing (en su totalidad) como Claude E. Shannon (por haber sido incomprendido desde las ciencias sociales). Al omitir o comprender erróneamente a dichos autores en las ciencias de la comunicación, también se ha ignorado a la comunicación secreta y a la criptografía computacional.

Sobre los modelos que estudian la comunicación, Karam (2005) comienza con el *libro blanco* (por el color de su encuadernación), publicado en 1982 por Martín Serrano *et al* [89] donde se hace una contribución epistemológica relevante de los modelos que pueden estudiar la comunicación y que desde su punto de vista presentan " una mirada integral que supera por mucho la visión maniquea del triunvirato (estructuralismo-marxismo-funcionalismo) en el que muchos nos (de)formamos. Cabe subrayar algo obvio –continuamos con Karam– que no siempre se considera en las clases de teoría (y epistemología) de la comunicación, que su estudio no puede restringirse a los medios, ni únicamente a sus estudios psico-sociales o socio-políticos" *(*Karam 2005: 9).

Como es sabido[90], el estudio sistemático de las ciencias de la comunicación emerge en Estados Unidos, en los años cuarenta. En América Latina se fundan las primeras escuelas de comunicación en los sesenta, con el antecedente de las escuelas de periodismo, particularmente a partir de la prensa, pero también emerge con nuevas perspectivas (como la cibernética), en un contexto acelerado de mundialización y de reorganización del campo académico (Karam 2005: 1).

[89] *C*on José Luis Piñuel, Jesús Gracia y María Antonia Arias, profesores del Departamento de Sociología IV de la Facultad de Ciencias de la Información en la UCM de Madrid.
[90] Véanse autores como Mattelart 1999) y el mismo Martín Serrano (1078 y 1982)

En la academia va surgiendo una reflexión cada vez más amplia sobre el fenómeno de la comunicación y su parte epistemológica. Como es reconocido por varios autores (Galindo, 2002), Wallerstein (1996) y el propio Martin Serrano (1989,1997), la comunicación (como centro de reflexión) surgió en escuelas de psicología, sociológica y ciencia política e incluso desde otras áreas como las artes y las humanidades (Fuentes Navarro (2004: 32). Ocurrió lo que varios académicos denominaron como la *sociologización de la comunicación* que le dio una cierta identidad. Cabe agregar que después de la segunda posguerra, el estudio de la comunicación comenzó a adquirir protagonismo con el *boom* de los estudios del enguaje (estructuralismo francés, Saussure[91]) y la preocupación creciente por la supremacía e injerencia de las nuevas tecnologías en todos los ámbitos de la vida.

Al sustentar si la comunicación posee el carácter de un saber sobre algo general que concierne a otras ciencias, Karam (2005: 4) plantea dos respuesta posibles: (a) que la comunicación es un saber integrador, es decir, que se entendería como un macrosistema para la organización del saber; o bien (b) que la comunicación sería un saber de los aspectos generales; es decir, de aquello que aparece en cualquier fenómeno sea natural o social.[92]

En ese sentido, Karam (2005: 5) retoma las preguntas que se hace Martín Serrano: "¿Existen las ciencias de comunicación como saberes específicos, diferenciados epistemológicamente de los saberes que aportan las otras ciencias?, ¿existe justificación teórica y necesidad práctica para que los estudios

[91] Véase F. de Saussure (1913).

[92] "El estatuto de la comunicación parece ser el de un saber que concierne a la física, pero no se deriva de ella ni de sus métodos; que le compete a la biología sin proceder de ella o de sus métodos; que puede tener nexos estrechos con la lingüística, la historia, la lógica, sin ser necesariamente una derivación de ellas ni depender de sus respectivos métodos. El analista y el epistemólogo de la comunicación no debe intentar alinearse a favor o en contra de la concesión de este estatuto; interesa examinar las razones por las cuales, precisamente en nuestra época, se quiere ver en la comunicación el saber integrador de las ciencias naturales y culturales. Al preguntarse sobre el cómo y para qué se genera un saber comunicativo, será la ocasión de comprender los rasgos que posee la producción de conocimiento en nuestra sociedad y en nuestro tiempo" (Karam, 2005: 5).

de la comunicación sean un saber independiente? Si esto fuera así, ¿dónde se ubican las ciencias de la comunicación, entre las lógicas, entre las ciencias naturales, culturales, sociales o están fuera? Para Martín Serrano hoy se tienen respuestas parciales a estas preguntas".

Como bien agrega este académico: "No debe extrañar que ninguno de los "padres fundadores" de la comunicología provenga de un campo ajeno a ello. Cuestiones que tenemos por específicas de la comunicación fueron examinadas y enumeradas por lingüistas, psicoanalistas, antropólogos, matemáticos, físicos: las interacciones comunicativas entre los seres vivos y más particularmente entre los seres humanos han sido estudiadas desde los orígenes de las ciencias sociales y naturales. El objeto materia ha estado ahí, lo que cambia ahora (y ese es uno de los principales retos epistemológicos) es el objeto formal, el enfoque". (Karam, 2005: 6). Pero en este enfoque se ha omitido retomar de las ciencias básicas (naturales) a la comunicación secreta y a la criptografía computacional hacia las ciencias sociales (específicamente la comunicación).

En los años sesenta o setenta del siglo pasado, por ejemplo, era improbable relacionar el concepto de comunicación surgido desde la semiología con el del emanado desde la cibernética. En ese contexto parecía necesario plantearse el estudio de la comunicación como un objeto específico y autónomo y proveerlo de consistencia teórica. De esa manera, "En el Siglo XX se proponen criterios sobre la naturaleza y el uso de la comunicación desde una pluralidad de campos del conocimiento. Participan muchas ciencias, lógico-epistemológicas, varias físicas y biológicas, todas las fisiológicas, sociológicas y culturales. En apariencia la comunicación puede parecer el coto troceado entre lingüistas, cibernéticos, psicoanalistas, cada uno tratando de demostrar la pertinencia de la comunicación. Martín Serrano ubica el último lustro de los sesenta como nodal en la búsqueda que varios estudiosos de formación científica variada realizaron sobre la naturaleza del objeto comunicativo. Cabe aclarar un pseudo-problema: La comunicación aparece en diversas ciencias porque el desarrollo del conocimiento

hace necesaria una reflexión sobre la información en casi todos los ámbitos…" (Karam, 2005: 7).[93]

Martín Serrano aclara un aspecto que podría parecer obvio pero que es preciso apuntar: el hecho de que la comunicación puede estar en muchos lugares pero no todo es comunicación; este pan-comunicacionismo es una actitud muy frecuente y de hecho tiene como antecedentes otras actitudes similares que acontecieron en la sociología y la psicología.[94]

Pasemos ahora a ubicar a los principales modelos de la comunicación desde las corrientes de análisis más utilizadas en nuestra área de estudio: el conductismo, el funcionalismo, el estructuralismo, el matemático y el sistémico. Cabe aclarar aquí que el modelo crítico-dialéctico merece mención aparte porque, desde nuestro punto de vista, no entra en aquellas corrientes y teorías de comunicación que podrían haber incluido dentro de sus postulados tanto a la comunicación secreta como a la criptografía computacional.

---

[93] "La necesidad de estudiar la comunicación se encontraba ya implícita cuando aparece en el desarrollo del conocimiento la idea que es posible un saber de objetos heteromorfos -el caso de la economía política que tiene en su objeto instituciones, ideas, bienes; o la psicología social que combina objetos de la sociología (instituciones grupos, visiones del mundo) y la psicología (afectos, instintos, cogniciones.)-, lo que sucede según Martín Serrano a mediados del Siglo XIX. En consecuencia, la diversidad de enfoques en la concepción de la ciencia de la comunicación no surge de la diversidad de ciencias en las que se trata; esa es una consecuencia de la naturaleza hetero-dimensional de la comunicación y no su causa. Las concepciones de la comunicación son distintas, porque son diferentes los campos que se desean integrar" (Karam, 2005: 7).

[94] Martín Serrano tiene un concepto de comunicación y de los fenómenos comunicativos que no proviene básicamente de la sociología o ciencia política, sino de la etología y las ciencias de la conducta. Para él la teoría de la comunicación se ocupa de los actores que participan en una relación comunicativa, de las materias que el actor (*Ego*) modifica de forma temporal o permanente; del trabajo expresivo a través del cual un actor hace relevante para el otro alguna materia; de las señales, del espacio que deben salvar estas señales, de los sistemas de acoplamiento, de las representaciones entre emisor-receptor (*ego-alter*). No existe la posibilidad de comunicar si el trabajo expresivo de *ego* y el trabajo perceptivo de *alter*, no están guiados por las representaciones. Para *ego*, la representación le permite relacionar la producción de determinadas expresiones con la introducción de determinados datos referidos a un objeto de referencia; para *alter* la representación le permite relacionar la asimilación de determinados preceptos con la invocación de un repertorio de datos que concierne a un objeto de referencia. Toda comunicación aporta datos de referencia para que en la interacción se susciten representaciones generales (accionales, cognitivas, intencionales); esas representaciones, para que sean eficaces a la hora de identificar los objetos de referencia, de pautar la interacción entre los agentes, tienen que ser completa (Martín Serrano *et al*, 1982: 167-170).

Recalcamos, pues, que para los fines de esta investigación, de las diferentes teorías y corrientes de estudio de las ciencias de la comunicación destacamos las que tendrían que haber tomado en cuenta a la comunicación secreta y a la criptografía computacional y que, además, están directamente relacionadas con sus escuelas: el modelo de aguja hipodérmica, la teoría de la "omnipotencia de los media" o modelo de Lasswell, el modelo de Shannon-Weaver, el modelo de Berlo, la Escuela de Palo Alto, la Escuela de Frankfurt, la Escuela de Birmingham y el *actuar comunicativo* de Jüngen Habermas. Hacemos un breve recuento de sus principales planteamientos, incluido el de Shannon-Weaver que tratamos a profundidad más adelante.

III.2. Desde el conductismo

El primer modelo de la comunicación es el **conductista,** que surge del estudio de la conducta animal con un a visión positivista. Parte del supuesto de que sólo puede hacerse ciencia de lo que se ve, siendo su forma de proceder causal, lineal y que se verifica en la comprobación. Parte de la existencia de ciertos estímulos (E) que generan, cuando están presentes, determinadas conductas (R) y que no las generan cuando están ausentes E>R (Karam, 2005: 9).

Modelo de Lasswell. El modelo de comunicación diseñado por el Profesor Harold D. Lasswell en 1948[95] es, como mencionamos anteriormente, un proceso simplificado en cuatro preguntas: **¿quién dice qué?,** análisis del contenido del enunciado sistemático a emitir; **¿por cuál canal?,** proponía el estudio de los medios disponibles; **¿a quién?,** a quienes, ya que el objetivo es alcanzar públicos amplios, regionales, masivos (aún no se consideraba el término audiencia y sus

[95] Harold Dwight Lasswell, (Estados Unidos 1902-1978) es considerado uno de los forjadores de las ciencias de la comunicación; se dedicó a analizar las técnicas de propaganda de la guerra mundial y el fenómeno del liderazgo político. Los medios de comunicación son, para él, el canal por el cual se difunden los mensajes propagandísticos. Publicó su modelo en 1948, en el artículo "Estructura y Función de la Comunicación de Masas", a través del cual pretendía explicar el comportamiento de las masas como la respuesta ante distintos estímulos. Se sitúa en un contexto político de entreguerras con el desarrollo de los aparatos propagandístico de la Unión Soviética y de la Alemania nazi, situación propicia para presuponer, a partir de principios conductistas, ciertos efectos de los medios masivos sin realizar indagaciones empíricas.

posibles segmentaciones), y **¿con qué efecto?,** básicamente en esos años perseguían un acatamiento al mensaje.

Dado que este modelo se desarrolló en tiempos de gran conmoción social, como lo fueron las dos guerras mundiales, eso influyó en su deseo de profundizar en la construcción de la comunicación propagandística, política, interiorizándose además, en el discurso periodístico y en la construcción de los enunciados religiosos. Se centró en el análisis de los alcances de esas comunicaciones, como discursos persuasivos con una búsqueda pre-definida de resultados perentorios y de alcance masivo.

El modelo de Lasswell, que se ubica sobre todo en el periodo de la segunda posguerra del siglo XX en Estados Unidos, fue de los primeros en proporcionar un programa de investigación para la comunicación y en internacionalizarse. Plantea, para Karam (2005: 10) "…un programa de estudios que delinea, tal vez por primera vez, los objetos principales de reflexión y estudio de la comunicación; si bien el modelo se inscribe en una preocupación socio-política no limita sus aplicaciones heurísticas a otros campos del saber". Se caracteriza por tratarse de un proceso, con simplicidad conceptual, con mensajes masivos y uniformes, de orden político, periodístico, religioso; una supuesta inteligencia del emisor y pasividad del receptor, considerado este último masivamente. No hay interacción y busca una reacción esperada, única.

Para los fines de nuestra investigación, vale la pena mencionar que Lasswell basó muchos de sus planteamientos en la teoría de la información de Shannon-Weaver pero ignoró las teorías criptográficas y de la comunicación secreta del primero y omitió completamente a Turing.

Modelo de David K. Berlo. En su libro *El proceso de la comunicación*, este académico expone en el año 1960 un modelo de comunicación que trascendió como SMCR, *source* (fuente), *message* (mensaje), *channel* (canal) y *receiver*,

(receptor), que trata de advertir el comportamiento personal, en el acto de comunicarse. En sus planteamientos principales hace expresa alusión a los sentidos, intercalándolos entre la fuente emisora y el receptor, no mencionado en los modelos precedentes.

Berlo menciona los elementos que componen el enunciado, el contenido en sí mismo, el tratamiento que se le ha dado a su construcción, el código que subyace y la consideración de "pack", en alusión al constructo-mensaje. Expone los sentidos, como canal de acceso, es decir sentidos del receptor, para percibir la comunicación. Con respecto al destinatario final del mensaje, el receptor, otorga a éste las mismas cualidades del emisor, habilidad, actitudes, sistema social y cultura, consideración que llevaría a pensar en la eficacia de la emisión-recepción, a posibilitar decodificar el mensaje al recibir el contenido con fidelidad, ya que E-R poseen las mismas cualidades constitutivas.

Berlo construye un modelo lineal de comunicación humana, donde tanto la fuente como el emisor poseen las mismas cualidades constitutivas; la señal enviada y la recibida deberían contener cierta fidelidad. Hay unidireccionalidad de la comunicación E-R, intercalando un mensaje y un canal; menciona los sentidos humanos como un canal, cualidad para recibir el mensaje y profundiza en los componentes del mensaje y su consideración como un constructo pero ignora también a la acomunicación secreta y a la criptografía computacional. La inteligencia continúa expuesta desde la fuente de emisión. El receptor es pasivo pues carece de interacción efectiva.

Modelo de la aguja hipodérmica. Parte de que en la comunicación de masas el medio actúa como una "aguja hipodérmica" con efectos o impactos directos e indiferenciados sobre los individuos supuestamente *atomizados*. En las guerras mundiales los ciudadanos eran considerados blancos indefensos; si una persona era alcanzada por las fuerzas de la propaganda, podía ser cambiada y controlada. (Schramm, Wilbur, 1978: 242). Esta teoría conductista encerraba contenidos

propagandísticos, idóneos para concienciar sobre el patriotismo y la necesidad de participar en las contiendas. “El principal elemento de la teoría hipodérmica es la presencia explícita de una teoría de la sociedad de masas, mientras que en su vertiente comunicativa opera complementariamente una teoría psicológica de la acción. También puede describirse el modelo hipodérmico como una teoría de y sobre la propaganda. Pronto se hizo evidente que la teoría bala no coincidía con los hechos, el público era obstinado. A veces tenía un efecto contrario al que se había querido y no se percibía cambio alguno” (Schramm 1978: 242).

Este modelo (no se trata de un proceso o de una teoría), parte de la comunicación masiva como un proceso unidireccional; del mensaje como una idea o concepto central desde el emisor, con un receptor pasivo y donde no hay interacción. Pero el académico Raymond Bauer y otros investigadores “ …demostraron que el público estaba lejos de ser pasivo; que iba buscando lo que quería de los medios de masas, interpretaba lo que respondiera a sus necesidades y predisposiciones y pocas veces cambiaba de opinión como resultado de la persuasión de masas. Hay una evolución desde la Teoría Bala al concepto del Público Activo”. (Mattelart 1999: 28). Aquí la comunicación secreta y la crptografía computacional así como Turing y Shannon también están ausentes.

Omnipotencia de los medios. Aunque algunos ejemplos del pasado[96] demostraron que la omnipotencia de los medios es posible frente a audiencias menos experimentadas en la percepción mediática, más sugestionables y en otras épocas, presas de una psicosis colectiva, en la actualidad la inteligencia de los receptores ha crecido frente a la múltiple exposición a sistemas de medios tan complejos y tan diversificados como los actuales.

[96] Es común citar, como ejemplo del poder de los media, el programa radial de la cadena CBS, de Estados Unidos, de Orson Welles, en el que describía, teatralizando, la novela “La Guerra de los Mundos” de H. G. Wells. Fue transmitido al aire en la noche del 30 de octubre de 1938, escenificando las imágenes descriptas en la novela, sobre una supuesta invasión marciana. Ese programa provocó estados de shock e histeria entre sus oyentes que seguramente hoy no se darían debido a la interacción del público con otros medios más inmediatos.

Pero los mensajes también han sido refinados en su técnica de presentación y exposición, pudiendo aún sugestionar y conmover a las audiencias, desde lo tecnológico, estratégico y táctico. “Por otra parte el poder de manipular las noticias según tendencias o ideologías a partir de las grandes corporaciones o grupos, posibilitan asegurar un flujo y penetración de las noticias y la información. Gobiernos y su aparato de difusión, editoriales, emisoras, canales y señales de televisión, de cable, de aire, satelital, agencias de publicidad, centrales de medios, logística de la distribución y circulación de la información, pueden manipular y asegurar hoy una omnipotencia de los media más allá del mensaje emitido” (Karam, 2005).[97]

III.3. Desde el funcionalismo

Los modelos surgidos a partir del funcionalismo también se originan en la biología y en el Siglo XIX se fundamentan a través de modelos evolucionistas, particularmente a través de biólogos sociales como el mencionado Spencer[98], quienes intentaron crear modelos sociales a partir de procesos naturales. Los estímulos que toma este modelo son aquellos que proceden de los "órganos de la sociedad" o les afectan. De esa manera, la fórmula unidireccional (E>R) se sustituye por otra (E<>R) (o bi-direccional).[99]

[97] “Idealmente en la comunicación se busca que el receptor se haga emisor y viceversa, eso se realiza mediante el llamado "*feedback*"; la comunicación se corresponde al *logo* de la linealidad: la respuesta del receptor coincide con la intención del emisor; algunas de las prácticas sociales de la comunicación que encarnan con más claridad esta aspiración son la publicidad y la propaganda, en donde queda muy clara esta razón instrumental con un recurso muy fuerte a la función persuasiva de la comunicación (*Cf*. Jakobson, 1981). Algunos sugieren que en un programa de radio cuando alguien habla, eso cumple las veces de "retroalimentación" , resume Karam (2005).

[98] El psicólogo, antropólogo y sociólogo inglés Herbert Spencer (Inglaterra, 1820-1903) desarrolló una concepción omnímoda de la evolución como el desarrollo progresivo del mundo físico, los organismos biológicos, la mente, la cultura humana y las sociedad. De él vale la pena revisar su texto *The Study of Sociology, que se encuentra en línea y otros sobre su obra como el de* Elliot, Hugh. *Herbert Spencer*. Londres: Constable and Company, Ltd., 1917 y Elwick, James. “Herbert Spencer and the Disunity of the Social Organism”, en *History of Science* No. 41, 2003.

[99] Karam (2005) explica que “Los componentes de este modelo son los órganos que cumplen una función (emisores), las funciones sociales que aseguran la estabilidad mediante el recurso de la comunicación, los órganos que cumplen las funciones de receptores, los medios, los mensajes funcionales (disfuncionales) y las respuestas (funcionales o disfuncionales)”.

Los componentes de este modelo se representan como los órganos que cumplen una función (emisores), las funciones sociales que aseguran la estabilidad mediante el recurso de la comunicación, los órganos que cumplen las funciones de receptores, los medios, los mensajes funcionales (disfuncionales) y las respuestas (funcionales o disfuncionales). Lo que busca el funcionalismo es el equilibro del sistema social y el uso que puede hacerse en su seno de la comunicación.

Ya apuntamos antes que idealmente en la comunicación se busca que el receptor se haga emisor y viceversa y que eso se realiza mediante la llamada retroalimentación; algunas de las prácticas sociales de la comunicación que encajan con más claridad en esta aspiración son la publicidad y la propaganda, en donde queda muy clara esta razón instrumental con un recurso muy fuerte a la función persuasiva de la comunicación (*Cf*. Jakobson, 1981).

Los primeros acercamientos teóricos que enmarcaron este modelo –que operó firmemente entre la primera generación de investigadores de la comunicación de masas en varias universidades estadounidenses– consistieron en justificar recuentos sobre las funciones de los medios de información. Uno de los más importantes lo realizó (tomando como base algunos aspectos del modelo de Lasswell de 1948) el sociólogo Charles Wright en 1960, quien planteó que los medios cumplen básicamente la función de vigilar el contexto social, ayudan a la interpretación de los hechos sociales y transmiten normas, valores culturales y entretenimiento y que dichas funciones son cubiertas de acuerdo a las características de los diferentes grupos sociales y los diversos niveles de la vida social.

III.4. Desde el estructuralismo

Por otro lado, los modelos estructuralistas parten del supuesto de que existen categorías universales que el conocimiento aplica a cualquier dato que proceda de

la realidad[100]. Los estructuralistas suponen la existencia de categorías que sirven como modelos para representar el mundo; incursionaron en el campo de la comunicación a través de la antropología y de la lingüística y se extendieron a través de las ciencias del lenguaje y el estructuralismo francés después de los años posteriores a la Segunda Guerra Mundial.[101] "Este modelo busca sobre todo conocer el código (sistema de reglas) para explicar la comunicación. El término estructura tiene muchas definiciones; en principio lo entendemos como un sistema de intercambios entre cualquier clase de actores sociales; en este modelo no interesa tanto qué es lo que se intercambia, ni quiénes; sino las reglas que aplican en sus relaciones".[102]

Vale la pena acotar que el estructuralismo aportó su preocupación por el lenguaje, sus sistemas y códigos y fue un poderoso instrumento para conocer los mensajes que emitían los medios. "Su labor más práctica –explica Karam (2005:12)– fue

[100]Los componentes del modelo son las relaciones de cambio, las reglas que explican dichas relaciones, los campos de aplicación en los cuales se aplica el código. Una de sus aplicaciones al campo de las ciencias humanas lo tenemos en la antropología estructural de Claude Lèvi-Strauss (*Antropología Estructural*, 1947), que intenta representar la forma como se da el intercambio de personas, bienes y signos en una sociedad, las "reglas" que explican tales o cuales movimientos, algún sistema determinado de intercambio, etc. El caso de la lengua natural es especialmente claro: el lingüista suizo Ferdinand de Saussure célebre por su *Curso de Lingüística General* (1913), concibe al lenguaje como un sistema de ajedrez y deja ver las bases del estudio sistémico y estructural de la lengua, la cual tiene todos sus componentes dentro de sí; desde esta contribución se ve al lenguaje como un sistema cerrado que posee todas sus instrucciones para comprensión y uso al interior de sí mismo; se supera las visiones históricas o comparativas para dar paso a una nueva forma de comprensión en este importante instrumento.

[101] "En el caso muy concreto del estructuralismo, esto fue importante en una etapa de la conceptualización de la comunicación; su preocupación por el lenguaje, sus sistemas y códigos vio en esta corriente de pensamiento un poderoso instrumento para conocer los mensajes que emitían los medios. Su labor más práctica dentro del mundillo de las escuelas de comunicación tan preocupadas del tema de los medios fue disponer a sus futuros egresados de sistemas para interpretar los mensajes, analizar la ideología subyacente o describir su estructura y modo de funcionamiento" (Karam, 2005: 11).

[102] Karam abunda: "Los componentes del modelo son las relaciones de cambio, las reglas que explican dichas relaciones, los campos de aplicación en los cuales se aplica el código. Una de sus aplicaciones al campo de las ciencias humanas lo tenemos en la antropología estructural de Claude Lèvi-Strauss (*Antropología Estructural*, 1947) que intenta representar la forma como se da el intercambio de personas, bienes y signos en una sociedad, las "reglas" que explican tales o cuales movimientos, algún sistema determinado de intercambio, etc. El caso de la lengua natural es especialmente claro: el lingüista suizo Ferdinand de Saussure célebre por su *Curso de Lingüística General* (1913), concibe al lenguaje como un sistema de ajedrez y deja ver las bases del estudio sistémico y estructural de la lengua, la cual tiene todos sus componentes dentro de sí; desde esta contribución se ve al lenguaje como un sistema cerrado que posee todas sus instrucciones para comprensión y uso al interior de sí mismo; se supera las visiones históricas o comparativas para dar paso a una nueva forma de comprensión en este importante instrumento".

disponer a s us futuros eg resados d e s istemas p ara i nterpretar los m ensajes, analizar l a i deología s ubyacente o describir s u es tructura y m odo de funcionamiento: es to s e hi zo m ediante s emióticas n arrativas al es tilo P ropp, Greimas y Bremond especialmente útiles en el estudio de los relatos y narrativas de algunos tipos de mensajes…". Aquí tampoco se toman en cuenta a Turing ni a Shannon; mucho menos a l a c omunicación s ecreta y a l a c riptografía computacional.

III. 5. Desde la teoría de la información

El primer artículo donde aparece resumido este modelo es *Una teoría matemática de la información* (1948) de Shannon-Weaver y representa un aprovechamiento de instrumentos m atemáticos y a ut ilizados en la t ermodinámica y en l a m ecánica estadística.

Modelo de Shannon-Weaver. El propio Karam y con él la mayoría de los teóricos de la comunicación con formación en el marxismo o en la teoría crítica, escriben sendos ens ayos y libros[103] criticando es ta t eoría has ta dejar de l ado l as aportaciones q ue s í hi zo S hannon a l a c omunicación pu es como pr ofundizamos más adel ante no de bemos pe dirle al go q ue no s e pr opuso (como el an álisis del contenido d e l a i nformación) y m ucho m enos hacerlo desde el punt o de v ista sociológico, ideológico o lingüístico).

Este m odelo s e c entró en medir la c antidad de i nformación matemáticamente soportada en un canal y la manera cómo se puede reducir el *ruido* (interferencia o pérdida d e l a i nformación) en la comunicación; s e ab ocó en l a t ransmisión de señales y en sus c omponentes: una fuente de i nformación, un t ransmisor, u n canal, una fuente de salida, un receptor y un destino. Tratando de justificarlo, "Uno puede c omprender es te m odelo –explica K aram 2 005: 10)– si s e pi ensa en l os esfuerzos d e S hannon y Weaver e n es e c ampo más dur o y di stante de l o q ue

[103] Véase los textos ya clásicos en las ciencias de la comunicación como aquellos de los Mattelart (1999), el propio Sánchez Ruiz y otros más recientes como el tan citado de Karam (2005).

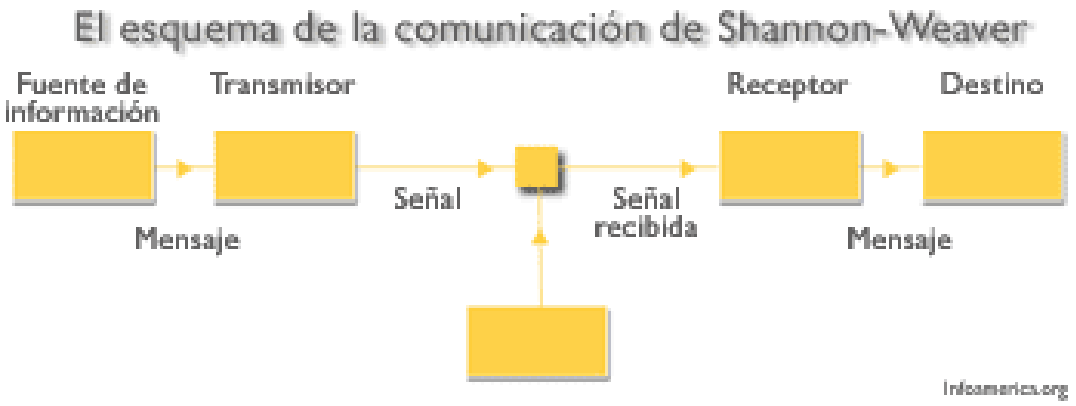
suele ser la reflexión social o cultural de la comunicación. El modelo matemático se aplica al estudio del intercambio de información entre máquinas; no hay problema epistemológico, en la medida que el proceso es cerrado. La concepción del proceso de comunicación es lineal y discurre entre un principio (fuente) y un final (destino) en donde queda cortada la transmisión".

Si bien su trabajo se definió como una teoría físico-matemática de la transmisión de la información, al hacerla medible hizo aportaciones a su comprensión desde el punto de vista técnico y contribuyó a facilitar su transmisión. Se suele diferenciar (y estamos de acuerdo con ello) entre un modelo de comunicación humana y un modelo de información, ya que ese aporte fue puramente matemático; de allí que en realidad creara una teoría matemática de la información, no de la comunicación desde el punto de vista social o antropológico.

En este modelo aparecen nuevos conceptos de gran utilidad para la transmisión de la información como los de fuente de información, el codificador que envía el mensaje a través del medio o canal y el concepto de ruido, es de cir, una interrupción o distorsión de la señal que llega a un decodificador, modificando en parte el mensaje o la posible interpretación del mismo al pasar al destinatario. En este modelo se prevé que el destinatario podría responder al estímulo recibido, aspectos que analizamos más a delante desde el ángulo específico de la hermenéutica profunda.[104]

De forma esquemática, este modelo se representó de la siguiente manera:

[104]"Programar supone además la incorporación de operaciones aritméticas y lógicas a las reglas de la operación mecánica, así como también reglas gramaticales e idiomáticas y comunicativas, etc. Para hacerlo se desglosan las operaciones en sus partes más elementales, ejecutándoselas una a una. En el modelo ideal de Turing se supone una máquina aislada enfrentada a una cinta muy larga (muchas veces descrita en la literatura especializada como "infinita"). Véase Flores Morador (2003).



Los términos presentes en este modelo, útiles para nuestra investigación, y que consideramos pertinente resaltar, son: **Fuente**, persona o conjunto de éstas, dispuestas a comunicarse con un objetivo determinado en forma de emisión de un mensaje. **Código**, conjunto de símbolos que incluye el mensaje desde la comunicación humana o tecnológica. **Codificador**, contenido tomado de la fuente, luego codificado, involucrando a la persona y sus formas de comunicar, sentidos, palabras, en sus diferentes expresiones, gestualidad o desde la tecnología propia de ese tiempo. **Canal**, conducto o medio, transportador del mensaje dirigido a un otro. **Ruido**, factor que de forma la construcción o calidad de la señal emitida, considerada como el mensaje, restándole fidelidad. **Decodificador**, en las comunicaciones humanas el receptor decodifica el mensaje enviado por la fuente emisora, más allá de poseer habilidades perceptivas e inteligencia, debe tener una cultura en común, un cierto nivel de conocimientos, con el emisor-codificador o fuente, para interpretarlo y comprenderlo.

Desde la teoría de la interpretación, podemos apreciar que este modelo plantea una teoría físico-matemática de la información; unidireccionalidad de la comunicación, aunque advierte una posible respuesta del destinatario; contempla un emisor considerado como "fuente" de información; describe un emisor-codificador y un receptor-decodificador del estímulo o señal. Los mensajes están codificados como estímulos o señales; describe un canal como soporte de comunicación y contempla un nivel de conocimiento del receptor (cultura en

común) para interpretar el mensaje pero es considerado pasivo, carente de interacción efectiva.[105]

Si bien este modelo se reconoce en las teorías de la comunicación, como lo hemos dicho ya y seguimos insistiendo, se le critica constantemente pues se asume que sus autores debían referirse también a la parte sociológica e interactiva de la Información, cuando ese no era su propósito. Sin embargo, hay que mencionar que la cibernética transformó este modelo lineal por otro circular, al introducir el concepto de *feed back* (retroalimentación) como mecanismo regulador del sistema.

Aquí cabe acotar que en sus planteamientos iniciales de la teoría de la información, el propio Shannon no hizo mención a la comunicación secreta ni a sus importantes investigaciones sobre criptografía pues, como lo mencionamos anteriormente, sus investigaciones criptográficas se mantuvieron secretas y fueron desclasificadas hasta años después de la segunda posguerra. Eso no justifica, por supuesto, que los modelos de comunicación posteriores y los teóricos de nuestra área de estudio hayan ignorado (y sigan ignorando) las importantes aportaciones de ese ingeniero estadounidense (y también de Alan Turing) a la comunicación secreta y a la criptografía computacional.

III.6. Desde la teoría de sistemas

Dentro de las denominadas teorías contemporáneas de la comunicación vale la pena retomar también otros aportes a la comunicación como el de Niklas Luhmann, con su Teoría General de Sistemas Sociales (TGSS) quien en 1968, inició un intenso debate teórico con Habermas, sobre el potencial que tiene la teoría de sistemas sociales [106]que continuó hasta la muerte de Luhmann en 1998.

[105] Aquí también cabría mencionar que Shannon proporciona un acercamiento a la comunicación ecrat y a la criptografía computacional que no se han tomado en cuenta en los estudios y modelos comunicativos.
[106] Luhmann escribió más de tres docenas de libros que abarcan temáticas referentes a leyes, economía, política, arte, religión, ecología, medios de comunicación y amor. Luhmann trabajó por "la gran teoría", apuntado a dirigir cualquier aspecto de vida social dentro de un marco universal teórico.

La teoría de sistemas (TS) fundamental los modelos sistémicos de la comunicación. Para Marín Serrano (1982), "La aportación de la TS consiste en señalar la necesidad de estudiar el objeto como un sistema que interactúa solidariamente con el medio ambiente (*Umwelt*); considera el sistema total como sistema productivo y reproductivo".

Escuela de Palo Alto. Los estudios sistémicos de esa Escuela se llevaron a cabo en la década de los años cuarenta y cincuenta en Estados Unidos. No tenían una sede que agrupara a sus investigadores por lo que también se les denominó *escuela invisible*. Sus integrantes analizaban las interacciones globales que involucraba a los seres humanos en la comunicación. Karam explica que se posicionaban en el ámbito investigativo inicial de las comunicaciones, (*Communicatión Research*) y los pioneros en esta dirección son el propio Lasswell, Wiener, Rosenblueth y von Bertalanffy a partir de su Teoría de los sistemas (1969); sistema abierto, intercambio e interacción.

Los autores de esta *universidad invisible* plantean algunos de sus principales postulados en el libro *La teoría de la comunicación humana* (*Cf*. Watzlawick *et al*, 1966), donde explican que los componentes básicos son los actores, los mensajes, las imágenes y los fines. Para esa época –continuamos con Karam– se rescataban cualidades de la cibernética, como *feed-back* o retroalimentación lo que, como se apuntó antes, transformó el modelo lineal en uno circular. La tendencia impuesta determinaba qué información debía poder circular, hacerse común, facilitando su intercambio. Los integrantes de Palo Alto profundizan, entonces, en la idea de que la comunicación no debe entenderse sólo como un flujo de acción y reacción, emisión del estímulo y reacción ante él, sino como un acto de intercambio, una interacción.

De esa manera, los principales aportes de la Escuela de Palo Alto a la comprensión de la comunicación son: "1) El principio de totalidad, que implica que un sistema no es una simple suma de elementos sino que posee características

propias, diferentes de los elementos que lo componen tomados por separado. 2) El principio de causalidad circular, que viene a decir que el comportamiento de cada una de las partes del sistema conforma parte de un complicado juego de implicaciones mutuas, de acciones y retroacciones. 3) El principio de regulación, que afirma que no puede existir comunicación que no obedezca a un cierto número mínimo de reglas, normas, convenciones. Estas reglas son las que, precisamente, permiten el equilibrio del sistema".[107] Si bien de gran relevancia para comprender el proceso de comunicación, todos estos aportes, también dejan fuera a Turing y a Shannon, a la comunicación secreta y la criptografía computacional.

III. 7. Desde la teoría crítica

Aunque es la más crítica hacia la teoría de la información y tampoco se ha acercado a la comunicación secreta y a la criptografía computacional, terminamos este capítulo con la teoría crítica, cuyos modelos crítico-dialécticos se aplican al análisis de los sistemas sociales a lo largo de la historia, y resultan de gran relevancia para la comprensión de los procesos comunicativos.

Entre los principales modelos crítico-dialécticos, debemos destacar al marxismo, cuyos " …postulados dan importancia a los componentes materiales de la vida social como factores para comprender el porqué de la transformación de las sociedades. En la estructura social hay una clase dominante que procura imponer a la comunidad una explicación de la naturaleza de la sociedad y la cultura que sirva a sus intereses y contribuya a la reproducción del sistema…". (Martín Serrano, *et al*, 1982: 123).

En *La ideología Alemana,* Karl Marx afirma que "las ideas de la clase dominante son, en todas las épocas, las ideas dominantes". Entre los enfoques marxistas tradicionales, destacan la teoría de la sociedad de masas teoría político-económica de los medios de comunicación; la teoría de la hegemonía de los

[107] Véase Wolf, Mauro (1996), Rizo, Marta (2004)y Marc, Edmond y Dominique Picard (1992).

medios de comunicación y la Escuela de Frankfurt, que describimos a continuación.

La teoría de la sociedad de masas destaca la interdependencia entre las instituciones que detentan el poder y sostiene que los medios de comunicación se integran a las fuentes de poder y a las autoridades sociales. En ese sentido, se considera que el contenido de los mensajes se encuentra al servicio de quienes poseen el poder político y económico y es posible ver en los mensajes mediáticos una interpretación irreal del mundo, de tal forma que, actuando como instrumento de manipulación, ayudan a las masas a sobrevivir en condiciones difíciles. Más allá de la teoría pesimista de la sociedad de masas, se encuentran las teorías de origen estrictamente marxista, que se diferencian de las anteriores por poseer un perfil ideológico más definido.

La teoría político-económica de los medios pone énfasis en la estructura económica por sobre el contenido ideológico de los mensajes. Los medios de comunicación se consideran parte del sistema económico estrechamente vinculado al sistema político. Los medios, bajo la presión de expandir sus mercados e impulsados por los intereses económicos de los propietarios, generan la necesidad de obtener beneficios propiciando tendencias monopólicas de integración vertical y horizontal. En consecuencia, se reducen las fuentes independientes y se marginan sectores minoritarios y de bajo nivel adquisitivo.[108]

Escuela de Frankfurt. Entre los teóricos de la Escuela de Frankfurt destacan Adorno, Horkheimer y Marcuse,[109] que trabajaron durante la Alemania de Weimar

[108] El filósofo, teórico marxista y político italiano Antonio Gramsci utiliza el término "hegemonía" para referirse a la cultura dominante, de esta forma, a muy grandes rasgos, puede describirse una segunda línea teórica dentro del marxismo, la cual no se centra ya en los determinantes económicos sino en la ideología misma, sus formas de expresión, sus sistemas de significación y los mecanismos a través de los cuales la clase oprimida, sobrevive en aparente conformidad, puesto que su conciencia se halla invadida y apta para la manipulación.

[109] Un grupo de investigadores seguidores de las teorías de Hegel, Marx y Freud ubicados en el Instituto de Investigación Social, inaugurado en 1923 en Fráncfort del Meno serían conocidos como Escuela De Frankfurt. También se les consideró representantes de la teoría crítica que se fundó ahí.

y fueron dispersados luego del ascenso de Adolf Hitler y del Nacional Socialismo al poder. Muchos de ellos continuaron su trabajo en Estados Unidos. La esencia de la teoría crítica de la Escuela de Frankfurt es conceptualizar la totalidad de las condiciones sociales y la necesidad de mejorarlas a partir de una comprensión de la situación histórico-cultural de la sociedad y de las contradicciones sociales. En sintonía con la teoría de la sociedad de masas, Marcuse explica que la sociedad es *unidimensional* y que su creación se debe a la *industria cultural*. Los medios de comunicación son, pues, un poderoso mecanismo que pretende contener el cambio que se vincula al modelo hegemónico". (Karam 2005).

Otros enfoques, como el sociocultural o **Escuela de Birmingham** están relacionados con los aportes de la Escuela de Frankfurt y otras escuelas de tradición humanista y de crítica literaria. La de Birmingham postula una visión realista de los productos de la cultura de masa en tanto que pretende comprender el significado y el lugar que ocupa la cultura popular dentro de las vivencias de los diferentes grupos sociales, la juventud, las minorías étnicas, la clase obrera, las clases marginales, etc. De esta forma, aspira a explicar el rol de la cultura de masas al integrar y someter a sectores sociales potencialmente inconformistas.[110]

Finalmente en este recuento –guiado por varios autores pero sobre todo por Karam (2005) y Martín Serrano (1999)– destacamos el *actuar comunicativo* del filósofo y sociólogo alemán Jürgen Habermas quien, en 1981, elabora su *teoría crítica del actuar comunicativo* y la sitúa dentro de la teoría sociológica, como una macro-teoría social. Aunque coincide en sus inicios con la Escuela de Frankfurt, se separa de ésta y relaciona los procesos macro-estructurales de la sociedad con los procesos micro-estructurales que involucran a los sujetos con objetivos propios

[110] Stuart Hall, representante de la Escuela de Birmingham, se opone al papel residual y meramente 'reflejo' asignado a lo cultural. Concibe a la cultura como formas normales del comportamiento humano y la define como los recursos y valores que surgen en los grupos sociales a partir de relaciones concretas en determinadas condiciones históricas mediante las cuales se 'manejan' y reaccionan las condiciones de la existencia. Quienes se ubican dentro de esta línea, aunque no son marxistas, coinciden en que las estructuras globales de la sociedad y las circunstancias históricas concretas son esenciales para comprender el funcionamiento de los medios de comunicación.

emanados en las experiencias personales, labradas en sus relaciones sociales, como parte de un intercambio simbólico, dentro del contexto del lenguaje.

Habermas hace aportaciones importantes al estudio de la comunicación pues "sitúa el grado de significación de la experiencia social de los sujetos claramente en las acciones de las personas, distinguiendo entre dos tipos de acciones fundamentales: acciones instrumentales estratégicas y acciones comunicativas. En éstas actúan los sujetos haciendo uso respectivamente de un tipo de racionalidad preferente (una racionalidad con respecto a fines y una racionalidad comunicativa). El reconocimiento explícito de una racionalidad comunicativa que se conceptualiza como aquella, en la cual se fundamentan, al mismo tiempo que se construyen, las intervenciones sociales relevantes de los sujetos, apunta a una interrelación significativa entre los elementos macro y macroculturales para las acciones humanas" (Philip, Rita Radl, 1998: 104). Su teoría del actuar comunicativo se orienta más a una teoría general de la sociedad, una mirada totalizadora, diferenciándose de una teoría social de una epistemología que analiza básicamente el comportamiento del individuo en la sociedad, que a la vez constituye.

Esos son, pues, los principales modelos, teorías y escuelas que van conformando los estudios e investigaciones en ciencias de la comunicación y que le van dan sustento y congruencia a nuestra área. Aunque en algunos de ellos –sobre todo en la teoría crítica– se dan aportes fundamentales al estudio de la comunicación desde el punto de vista sociológico y antropológico, en ninguno de ellos se da un lugar o se contempla desde la sociedad a la comunicación secreta y a la criptografía computacional, partes fundamentales de los procesos comunicativos de hoy. En ninguno de ellos se toma en cuenta a Turing y sólo en algunos se retoman los modelos matemáticos de Shannon. Como vimos, a Turing se le ignora totalmente y a Shannon se le critica y, en el mejor de los casos, se le cuestiona por no haber tratado aspectos sociológicos y de las entonces nacientes ciencias

de la comunicación que escapaban de su interés y área de estudio en la ingeniería computacional.

En los siguientes capítulos veamos el desarrollo de las TIC y de la criptografía computacional para analizar posteriormente qué tanto ambos teóricos se conocieron y compartieron no sólo un tiempo y una problemática sino sus conocimientos y aportaciones en la comunicación secreta primero y posteriormente en la criptografía computacional, en las ciencias de la comunicación y en el desarrollo de las tecnologías de la información y la comunicación.

CAPÍTULO IV

Las tecnologías de la información y la comunicación en el contexto sociohistórico del siglo XX

Si seguimos con el análisis sociohistórico y su ubicación espacio-temporal acotados por Thompson (2003) y reforzados por Aguirre Rojas (2004), no podemos dejar de mencionar algunos momentos clave en la historia de la ciencia y la tecnología del siglo pasado en relación a las TIC, otra de nuestras categorías principales.

IV.1 Las TIC y su desarrollo entre guerras

Comenzamos este apartado con una cita de Koofi Annan (2003), ex secretario general de la Organización de las Naciones Unidas que si bien es poco crítica, plantea un lado positivo del tema en cuestión y que dice lo siguiente: " Las tecnologías de la información y la comunicación no son ninguna panacea ni fórmula mágica, pero pueden mejorar la vida de todos los habitantes del planeta. Se dispone de herramientas para llegar a los Objetivos de Desarrollo del Milenio, de instrumentos que harán avanzar la causa de la libertad y la democracia y de los medios necesarios para propagar los conocimientos y facilitar la comprensión mutua".[111]

Desde el nacimiento de la ciencia moderna en el siglo XVII, el progreso científico se dio de forma continua pero fue en el siglo XX cuando la investigación y la aplicación técnica de los conocimientos científicos se desarrollaron a un ritmo tan acelerado que en pocas décadas han transformado radicalmente nuestra forma de vida. En los últimos años del siglo XX (y agregaríamos, las primeras décadas del siglo XXI) se han realizado más descubrimientos que en el resto de la historia de

[111] Discurso inaugural de la primera fase de la WSIS, Ginebra, Suiza.

la humanidad y la incorporación de principios científicos a tecnologías aplicables a la vida cotidiana se está produciendo a una velocidad vertiginosa.[112]

Si partimos del punto de vista del desarrollo tecnológico, la primera mitad del siglo XX se caracterizó por el empleo de las fuentes energéticas anteriores (como el carbón), el desarrollo adicional de la electricidad industrial y la intención de dominar la energía atómica. En este periodo, las principales innovaciones tecnológicas se dieron en la industria, la invención reciente de aparatos domésticos, la obtención de nuevos materiales de construcción como el hormigón armado y el cristal, de fibras sintéticas para la producción textil y de accesorios plásticos; en medicina, la penicilina y otros antibióticos; la mejora de los conocimientos en agricultura, alimentación y técnicas de conservación de alimentos; en el transporte, la producción en serie del automóvil, que se convirtió en el medio predominante de locomoción, la invención del aeroplano; en los medios de comunicación el desarrollo de la radiodifusión y de la cinematografía así como, en los años veinte, de la televisión creada a partir del invento del cinescopio.[113]

En el siglo XX el progreso científico estuvo cada vez más ligado al progreso técnico que, a su vez, constituyó uno de los principales motores del crecimiento económico. La ciencia amplió enormemente sus campos de investigación. El desarrollo, por ejemplo, de la estadística y de la informática, permitió transformar radicalmente los métodos de cálculo y de análisis. Pero la acumulación del saber y la cultura adquirida a lo largo del desarrollo de la humanidad, puesta en función de la industria bélica, específicamente durante la Primera y Segunda Guerras Mundiales, tuvieron un gran impacto en todos los ámbitos de la vida social así

[112] En el libro *Por los senderos de la ciencia,* el físico y divulgador de la ciencia Constantino Armestos (1995) sostiene atinadamente que en la actualidad hay más personas dedicadas a la ciencia que en toda la historia de la humanidad.

[113] Véase el capítulo 1, Balance crítico del siglo XX histórico. ¿Breve, largo o muy largo siglo XX?", de *Para comprender el siglo XXI,* Ediciones de Intervención Cultural/El viejo Topo, España, 2005, p. 26. Véase Aguirre Rojas (2004, 26-27), Marc Bloch (1996), Braudel (1991) y Hobsbawm (1994).

como un acelerado desarrollo de la ciencia y la tecnología. Una de las consecuencias tecnológicas inmediatas de ese desarrollo fue el surgimiento de las TIC, en las que profundizamos más adelante en este capítulo.

Las TIC están cambiando la forma tradicional de hacer las cosas. La primera generación de computadoras, debidas precisamente al trabajo de Turing, Shannon y otros matemáticos e ingenieros, se destinó a guardar los registros y monitorear el desempeño operativo bélico, empresarial y académico, pero la información no era oportuna o inmediata. Los avances actuales hacen posible capturar y utilizar la información en el momento que se genera, es decir, lo que se denomina hoy como *procesos en línea*. Este hecho no sólo ha cambiado la forma de realizar el trabajo y el lugar donde realizarlo sino que también ha tenido un gran impacto en la competencia y la generación y transmisión de la información.[114]

IV.2. La computación en una nueva era

Además de caracterizar a las TIC, en este apartado ubicamos la enorme importancia que tiene hoy la computadora para el desarrollo de todas las áreas de la vida, pero vayamos por partes. Para ubicar la gran cantidad de avances científico-tecnológicos del momento vale la pena volver al texto del reconocido escritor, profesor en la Universidad de Warwick y miembro de la Royal Society de Gran Bretaña, Ian Stewart quien está convencido de que las ***ecuaciones*** son el alma de las matemáticas. Sin ellas –explica– nuestro mundo no existiría, pues aunque tengan la fama de ser *horripilantes*, la historia de la humanidad se ha redirigido varias veces gracias a una ecuación; éstas tienen poderes escondidos, revelan secretos de la naturaleza.[115] De este autor retomamos una de las 17

[114] Véase Atiar, Rahman, "Conceptos fundamentales y lista", stretdirectory.com., 2009. Las TIC (unión de los computadores y las comunicaciones) desataron una explosión sin precedentes de formas de comunicarse al comienzo de los años 90 del siglo XX. A partir de ahí, Internet pasó de ser un instrumento especializado de la comunidad científica a ser una red de fácil uso que modificó las pautas de interacción social.

[115] Para Ian Stewart "El poder de las ecuaciones recae en la correspondencia filosóficamente difícil entre las matemáticas, una creación colectiva de mentes humanas, y una realidad externa física. Las ecuaciones dan forma a patrones profundos en el mundo exterior". Stewart nos invita a valorar las ecuaciones y sus símbolos en toda su dimensión, a conocer sus fascinantes historias para descubrir nuestro mundo. Está convencido de su importancia para la ciencia y la tecnología. De manera didáctica, las divide en dos grupos:

ecuaciones que cambiaron al mundo y entre las que se encuentra, además de la de Einstein, la de la Teoría de la información de Shannon. (Stewart, 2015).

De acuerdo a nuestras categorías de **espacio-tiempo, ciencia-tecnología** y que con Thompson "El objetivo del análisis sociohistórico es reconstruir las condiciones sociales e históricas de la producción, la circulación y la recepción de las formas simbólicas"[116], los hechos más relevantes en cuanto al desarrollo de la computación, en nuestro siglo corto y el mundo anglosajón, además de los avances mencionados en el capítulo II, destacan los siguientes. [117]

En 1906, por ejemplo, se inventó el tubo de vacío (o *Audion*) que constaba de una bombilla de vidrio con la que se podían recibir y amplificar señales de radio de una antena; en 1919 se creó el primer circuito multivibrador o biestable (*flip-flop*) que permitió diseñar circuitos electrónicos estables, alternativamente, pudiendo representar así el 0 como un estado y el 1 con el otro. Esto fue fundamental para el almacenamiento y proceso del ***bit binario,*** estructura que utilizan desde entonces las computadoras. Años más tarde, en 1925, en Estados Unidos, se fundaron los Laboratorios Bell, como hemos mencionado, centros de importantes avances en matemáticas, criptografía, ingeniería y computación.

Cinco años después, en 1930, el reconocido matemático Vannevar Bush construyó una máquina diferencial parcialmente electrónica, capaz de resolver ecuaciones diferenciales y en 1931, Kurt Gödel, otro destacado matemático,

---

las que revelan regularidades matemáticas y aquellas que expresan leyes de la naturaleza. Muestra qué nos dice cada una, por qué son importantes y lo que provocó enunciarlas. Comienza con el Teorema de Pitágoras, los logaritmos (para cortar procesos), el cálculo, la Ley de la Gravitación Universal, la raíz cuadrada de menos uno y la distribución normal (patrones al azar). Sigue, entre otras, con las ecuaciones de Maxwell, la Segunda Ley de la Termodinámica (y el desorden), la relatividad y otras entre las que se encuentra una de nuestro particular interés, la Teoría de la Información (códigos, comunicaciones y ordenadores) de Shannon. Stewart (2015) y Valek (2016).

[116] "La formas simbólicas son producidas (expresadas, actuadas, inscritas) y recibidas (vistas, escuchadas, leídas) por individuos situados en ubicaciones específicas, que actúan y reaccionan en momentos y lugares particulares, y la reconstrucción de estos lugares es una parte importante del análisis sociohistórico". *Ibídem*, Thompson, p. 409.

[117] Diversos textos narran la historia y el desarrollo de la computación y las computadoras; entre ellos el de Davis, Martin (2000): *Engines of Logic Mathematicians and the Origins of the Computer*, Norton.

publicó un documento sobre los lenguajes formales basados en operaciones aritméticas, cuyos resultados fueron fundamentales para la teoría matemática de la computación.

En 1936 Alan Turing describió la denominada ***máquina de Turing***, que caracteriza formalmente el concepto de **algoritmo** y en la que profundizaremos en el capítulo VI. Cuatro años después, Konrad Zuse completó la primera computadora electromecánica, la Z1, que fue la primera máquina programable y completamente automática.

Siguiendo con los principales avances durante nuestra división del siglo corto, en 1938 se desarrolló la primera generación de computadoras compuestas con tubos de vacío, que abarcadas desde 1938 hasta 1958, cuando surgió la segunda generación de ellas. En 1939 los ingenieros William Hewlett y David Packard fundaron en Palo Alto, California la compañía Hewlett-Packard y en plena Segunda Guerra Mundial, 1940, Samuel Williams y George Stibitz completaron en los Laboratorios Bell una calculadora electromecánica que podía manejar números complejos. En 1942, John Vincent Atanasoff y Clifford Edward Berry crearon una calculadora de propósito especial para resolver sistemas de ecuaciones lineales simultáneas, la cual fue llamada "ABC" (*Atanasoff Berry Computer*) y en 1944, se construyó, en la Universidad de Harvard, la *Harvard Mark I* (primera máquina electromecánica), diseñada por un equipo encabezado por Howard H. Aiken.

Mientras, en Inglaterra, también en 1944, Turing participó en la construcción de las computadoras Colossus (*Colossus Mark I* y *Colossus Mark 2*), con el objetivo específico de descifrar las comunicaciones alemanas durante la Segunda Guerra Mundial. En 1945 el matemático húngaro-estadounidense John von Neumann describió el diseño lógico de una computadora utilizando el concepto de programa almacenado (*stored-program*).[118] Como mencionamos en páginas precedentes, usó una arquitectura distinta, hoy conocida como *Arquitectura de von Neumann*.

[118] Se trata del "*First Draf of a Report on the EDVAC*" una página del primer documento.

Ese mismo año Vannevar Bush desarrolló la teoría de Memex, un dispositivo de hipertexto ligado a acervos de libros y películas.

Ya en la posguerra, en 1946, en la Universidad de Pensilvania se construyó la ENIAC (*Electronic Numerical Integrator And Calculator*), que ha sido considerada como la primera computadora electrónica de propósito general.[119] Vale la pena detenernos un poco en sus características pues la máquina ocupaba todo un sótano de la Universidad, tenía más de 17,000 tubos de vacío, consumía 200 kW de energía eléctrica, requería todo un sistema de aire acondicionado y tenía la capacidad para realizar 5 000 operaciones aritméticas por segundo.

También, en 1946, pero en Europa, se puso un funcionamiento la computadora británica EDSAC (*Electronic Dilay Storage*) construida por Maurice Wilkes y un equipo perteneciente al Laboratorio de Matemáticas de la Universidad de Cambridge, inspirada en algunas de las ideas de von Neumann y los avances en computación de Turing.

En 1949 Jay Forrester desarrolló la primera memoria, que reemplazó a los tubos al vacío (***bugs***) como la forma predominante de memoria para la siguiente década. Ese mismo año, la computadora EDSAC corrió su primer programa. Como ya lo hemos mencionado y seguimos profundizando, en 1950 Alan Turing describió lo que ahora se conoce como la *prueba de Turing*, donde exploró el desarrollo natural y potencial de la inteligencia y la comunicación humana y de computadoras. En 1951 comenzó a operar la EDVAC que, a diferencia de ENIAC, no era decimal, sino binaria y tuvo el primer programa diseñado para ser almacenado. Ese mismo año, se utilizaron las primeras computadoras electrónicas en las oficinas de censos estadounidenses.

[119] Hay varios textos sobre cuál fue en realidad la primera computadora digital. Uno que vale la pena revisar es *La catedral de Turing*, de George Dysson, donde defiende la primicia de Von Neumann sobre la primera computadora.

Como mencionamos en el capítulo II , en 1952 Claude E. Shannon desarrolló el primer ratón eléctrico capaz de salir de un laberinto, considerado como la primera red neural. Un año más tarde, en 1953, la compañía IBM fabricó su primera computadora a escala industrial, la IBM 650 ; se amplió el uso del lenguaje ensamblador para la programación de las computadoras y ese mismo año se crearon memorias de núcleos magnéticos.

En 1954 se dio a conocer el primer lenguaje de programación de alto nivel Fortran. De ahí en adelante el desarrollo de las computadoras y sus programas ha sido fugaz y exponencial; sólo añadiremos por ahora que, en 1956, nació formalmente el área de investigación de la ***inteligencia artificial***.[120] En 1958 comenzó la segunda generación de computadoras, caracterizadas por usar circuitos transistorizados en lugar de válvulas al vacío. En 1960 se desarrolló COBOL, el primer lenguaje de programación de alto nivel transportable entre modelos diferentes de computadoras. Se creó el primer glosario de computador y C. Antony R. Hoare diseñó el ***algoritmo*** de ordenamiento o clasificación llamado *quicksort*. Los avances posteriores son otra historia que rebasa los objetivos de este trabajo de investigación.[121]

Después de esta fugaz revisión historiográfica alrededor de la computación y las TIC, en el siguiente apartado nos referimos puntualmente a su desarrollo para después situar la conexión entre Alan Turing y Claude Shannon con respecto a la criptografía y la computación y su papel en la Segunda Guerra Mundial. Además de continuar con su ubicación sociohistórica, comenzamos a delimitar las otras dos fases o procedimientos principales que comprenden la hermenéutica profunda; es decir, las dimensiones analíticamente distintas del proceso

[120]Se dictó una conferencia a partir de la cual comenzó a usarse el término y al cual contribuyó el propio Shannon. Véase Davis (2000).

[121] En 1956 Edsger Dijkstra formuló un algoritmo eficiente para descubrir las rutas más cortas en grafos como una demostración de las habilidades de la computadora ARMAC. En 1957 IBM puso a la venta la primera impresora de matriz de puntos; se fundó la compañía Fairchild Semiconductor y Jack S. Kilby construyó el primer circuito integrado.

interpretativo, explicadas por John B. Thompson (2010): el análisis formal o discursivo y la interpretación/reinterpretación. (Bologna, J. y Walsh, A. M., 1997).

Con respecto al análisis formal o discursivo, sólo mencionamos –sin profundizar pues escapa a los objetivos de esta investigación– las aportaciones de Turing y de Shannon (como significantes y a su obra, como significados, en el nivel diacrónico) para desencriptar una serie de códigos; decodificar de una esfera semántica a otra revelando lo que los alemanes querían mantener en secreto a partir de teorías matemáticas. A reserva de profundizar más adelante en el capítulo VI, por lo pronto diremos que Turing descifra los mensajes alemanes de guerra mientras que Shannon establece las condiciones necesarias para que una señal pueda transmitirse de manera precisa y confiable y explica la forma y cantidad de esa información que llega a su destinatario.

IV.3. ¿Nuevo paradigma?

En términos generales definimos a las TIC como las herramientas y métodos empleados para recabar, retener, manipular o distribuir información, generalmente asociadas con las computadoras y las tecnologías afines aplicadas a la toma de decisiones. (Bologna, J. y Walsh, A. M., 1997). Las TIC han transformado y siguen cambiando la forma de hacer las cosas. La primera generación de computadoras estaba destinada a guardar los registros; hoy es posible capturar y utilizar la información en el momento que se genera, es decir, tener procesos en línea. (Alter, 2008).

En los años noventa del siglo pasado, la unión de las computadoras y las comunicaciones (TIC) desató una explosión sin precedentes de formas de comunicarse. A partir de ahí, las redes digitales, específicamente Internet pasó de ser un instrumento especializado de la comunidad científica a ser una red de fácil uso que modificó las pautas de interacción social pues las nuevas tecnologías de la información y comunicación no sólo designan al a vez un conjunto de

innovaciones tecnológicas sino también las herramientas que permiten una redefinición radical de interacción de la sociedad.

Como lo han explicado académicas como Alva de la Selva (2015), las TIC se deben, entre otras cosas, a la creación del idioma de la informática, el lenguaje digital. "En sentido amplio, se entiende por digital cualquier indicación numérica realizada con cifras; sin embargo, en el proceso electrónico de datos ese término se refiere exclusivamente a cualquier representación en *sistema binario*." (Alva de la Selva, 2015: 24). Ya no se transmite analógicamente una señal sino que se hace en forma *codificada, cifrada*.

Atinadamente, Alva de la Selva caracteriza a las TIC a partir de sus propiedades básicas como la digitalización, la interactividad, la instantaneidad, la interconexión, la flexibilización y la innovación. Así "El desarrollo de la digitalización ha permitido reducir a un mismo denominador técnico común [unos y ceros] todos los servicios y redes, para permitir no sólo un procesamiento y almacenamiento efectivos de la información, sino además tener al alcance la posibilidad de ejecutar la transmisión de las señales codificadas a mayores velocidades". (Alva de la Selva, 2015, 25) Algunos ejemplos de estas tecnologías son la pizarra digital, la computadora personal, el proyector multimedia, los *blogs*, el *podcast* y, por supuesto, la *web*.

La misma autora retoma la definición de telecomunicaciones como redes de comunicación alámbricas, inalámbricas o en microondas, que llevan información (ya sea voz, datos, televisión, o servicios agregados de cómputo) de un punto a otro sin intervención editorial. En su afán por identificar y clasificar el ámbito de las TIC, la investigadora y catedrática de la UNAM las clasifica en *redes* (telefonía fija y móvil, banda ancha, redes de TV y en el hogar); *terminales* (computadoras, internet, reproductores portátiles de audio y video, TV), y *servicios* (correo electrónico, banca online, música, cine, TV, blogs, servicios móviles, etc.). (Valek, 2016-II).

De esa manera, para los fines de esta investigación, retomamos a las TIC o nuevas tecnologías de la Información y comunicación son aquellas herramientas computacionales e informáticas que procesan, almacenan, sintetizan, recuperan y presentan información. Fungen como soportes y canales para el tratamiento y acceso a la información para dar forma, registrar, almacenar y difundir contenidos informacionales.

Planificar y gestionar la infraestructura de las TIC es una labor compleja que requiere una base sólida de la aplicación de los conceptos fundamentales de las ciencias de la computación. Se requieren habilidades especiales en la comprensión, por ejemplo, de cómo se componen y se estructuran los sistemas en red. En sistemas de información hay importantes aspectos de *software* como la fiabilidad, seguridad, facilidad de uso y la eficacia y eficiencia para los fines previstos. (ACM, 2014).

Así, los profesionales de las TIC combinan los conocimientos, prácticas y experiencias para atender tanto la infraestructura de tecnología de información de una organización como las personas que lo utilizan. Integran los productos con las necesidades y la infraestructura organizativa, instalación, adaptación y el mantenimiento de los sistemas de información, proporcionando así un entorno seguro y eficaz que apoya las actividades de los usuarios del sistema de una organización. En las TIC la programación a menudo implica escribir programas que normalmente se conectan a otros programas y a existentes. *(Computing Degrees and Jobs*, 17 de Julio de 2014).

IV. 4. Concepto dinámico de las TIC

En tanto tecnologías que favorecen la comunicación y el intercambio de información, el teléfono, la televisión y la computadora forman parte de las TIC (Lyne Markus y Daniel Robey, 2009). Los primeros pasos hacia una sociedad marcada por la información estuvieron dados por el telégrafo eléctrico, después por la radiotelefonía, la televisión y posteriormente por la computadora e Internet.

La telefonía móvil y el GPS han asociado la imagen al texto y a la palabra sin cables. Internet y la televisión son accesibles en el teléfono móvil, que es también una máquina de hacer fotos. *(Evolución tecnológica*, 2009).

En la última década del siglo XX, la asociación de la informática y las telecomunicaciones se ha beneficiado de la miniaturización de los componentes, permitiendo producir aparatos *multifunciones* a precios accesibles desde el año 2000. El uso de las TICs sigue extendiéndose, sobre todo en los países desarrollados, con el riesgo de acentuar localmente la brecha digital y social y la diferencia generacional. (*Brecha digital*, 2009).

Las TIC ocupan hoy en día un lugar creciente en nuestra vida cotidiana. (Lista de referencias sobre TIC, 2009): desde la agricultura de precisión hasta la monitorización global del medio ambiente, pasando por el comercio, la telemedicina, las bases de datos, la bolsa, la robótica y los usos militares, sin olvidar la ayuda a los discapacitados (por ejemplo, débiles visuales que usan sintetizadores vocales avanzados).

Hoy en día estamos inmersos en la llamada *sociedad de la información, a la que* entenderemos como aquella en la cual las tecnologías facilitan la creación, distribución y manipulación de la información y desempeñan un papel esencial en nuestras actividades.[122] Ella se debe principalmente a Internet, que apareció en 1969 y, como mencionamos, se gestó como parte de la Red de la Agencia de Proyectos de Investigación Avanzada (ARPANET), del Departamento de Defensa de Estados Unidos. Sus principios básicos consistían en ser una red descentralizada con múltiples caminos en tre dos puntos y que los mensajes estuvieran divididos en partes que serían enviadas por caminos diferentes. La presencia de diversas universidades e institutos en el desarrollo del proyecto hizo

[122] El concepto comenzó a utilizarse en Japón durante los años sesenta, considerándose al autor Yoneji Masuda como su divulgador, a partir de una obra publicada en 1968. Manuel Castells examina los caracteres de ese paradigma para acuñar el de *era informacional*, con Internet como fundamento principal a este nuevo modo de organización social en esferas tan dispares como las relaciones interpersonales, las formas laborales o los modos de construir la identidad propia.

que se fueran encontrando más posibilidades de intercambio de información. Posteriormente se crearon los correos electrónicos, los servicios de mensajería y las páginas web. Pero fue hasta mediados de la década de los noventa (cuando había dejado de ser sólo un proyecto militar) que se dio la verdadera expansión de Internet. (Atiar Rahman, 2009).

El desarrollo de Internet implica que la información esté ahora en muchos sitios. Antes la escuela y la universidad eran los ámbitos que concentraban el conocimiento. Hoy se han roto barreras y con Internet hay mayor y más rápido acceso a la información. También se ha agilizado el contacto entre personas con fines sociales y de negocios. No hace falta desplazarse para cerrar transacciones comerciales en diferentes ciudades del mundo en forma rápida y eficaz; el principal problema es la *calidad de esa información.*

En cierta medida, estas nuevas tecnologías son inmateriales, ya que la materia principal es la información; permiten la interconexión y la interactividad; son instantáneas; tienen elevados parámetros de imagen y sonido. Al mismo tiempo las nuevas tecnologías suponen la aparición de nuevos códigos y lenguajes, la especialización progresiva de los contenidos sobre la base de la cuota de pantalla (diferenciándose de la cultura de masas) y dando lugar a la realización de múltiples actividades en poco tiempo. (Desmitificando las TIC, 2009).

El concepto de TIC presenta dos características típicas de las nociones nuevas: es frecuentemente evocado en los debates contemporáneos y su definición semántica queda borrosa y se acerca a la de la sociedad de la información. (Borrosidad semántica, 2009). El advenimiento de Internet y principalmente de la *World Wide Web* como medio de comunicación de masas y el éxito de los *blogs*, las *wikis* o las tecnologías *peer-to-peer* confieren a las TIC una enorme dimensión social.

Antes de profundizar en las características técnicas de las TIC, resumamos algunos de los momentos clave en su desarrollo. Según un recuadro[123] ampliamente difundido en el mundo anglosajón y especialmente estadounidense, los momentos clave en la historia de las TIC, ocurren en 1946, con ENIAC, la primera máquina considerada una computadora, con un peso de 30.000 kg y que operaba con válvulas y circuitos de acuerdo con cada función. En 1951 nace UNIVAC, el primer ordenador comercial con un peso de 7.000 kg y 1Kb de memoria y funcionaba con válvulas de vacío. En 1953 IBM crea la serie 701 y vende 18 unidades por el mundo. El segundo momento ocurre cuando aparecen los sistemas operativos que permiten ejecutar distintos programas a la vez mediante el uso simultáneo de varios procesadores. El tercero, en 1961 cuando se publica la teoría de disminución de paquetes de información; un año después se sustituyen las válvulas por transistores con las mismas funcionalidades pero ahorrando espacio. El cuarto momento ocurre en 1965 cuando L. G. Roberts en el MIT conecta dos computadoras a una base telefónica y en 1966 desarrolla las bases teóricas para crear la red ARPANET y sigue el desarrollo con las siguientes etapas hasta que los transistores se sustituyen por circuitos integrados y se avanza en la liberación de tecnología de ellos en las computadoras personales. (*Creative Commons s.f.).* Hasta aquí mencionamos los momentos más trascendentes pues los siguientes ocurren en la segunda mitad del siglo XX y escapan a los objetivos de esta investigación. La historia británica es diferente y la vemos en los siguientes capítulos.

IV.5. Características y accesibilidad de las TIC

Las TIC conforman un conjunto de recursos necesarios para manipular la información: las computadoras, los programas informáticos y las redes para convertirla, almacenarla, administrarla, transmitirla y encontrarla. Su estudio y ubicación se facilita si las clasificamos según las redes, las terminales y los servicios.

[123] Véanse los "10 momentos clave en la historia de las TIC" (*Creative Commons,* s.f.)

Las principales redes de acceso disponibles son la telefonía fija (con el uso de un módem en un acceso telefónico básico[124]; banda ancha.[125] e Internet que está aumentando la cantidad de contenidos pesados (videos, música).[126]

Las primeras tecnologías que permitieron el acceso a datos, aunque a velocidades moderadas, fueron el GPRS y el EDGE, ambas pertenecientes a lo que se denomina 2.5G. (González Ortiz, 2008). La evolución del teléfono móvil permitió disminuir su tamaño y peso y comunicarse desde casi cualquier lugar.[127]

Actualmente hay varias tecnologías para la distribución de contenidos de televisión, incluyendo las versiones analógicas y digitales: la terrestre o método tradicional de enviar la señal de televisión, en forma de ondas de radio por el espacio abierto. La televisión por cable, en la que se transmiten señales de radiofrecuencia a través de fibras ópticas o cables coaxiales, y la televisión por Internet que traduce los contenidos en un formato que puede ser transportado por redes IP y conocida, por ello, como televisión IP.

Cada día hay más dispositivos con algún tipo de conectividad.[128] Hay gran cantidad de servicios de valor añadido disponibles que incluyen desde servicios relacionados con el entretenimiento, la posibilidad de jugar en línea y multimedia hasta servicios de salud o educativos. (McManus, 2008).

---

[124]Véase "La sustitución de los teléfonos fijos sigue acelerándose", 2007.

[125] Según la Comisión Federal de Comunicaciones de Estados Unidos (FCC) se considera banda ancha al acceso a una velocidad igual o superior a los 200 kbit/s, como mínimo en un sentido. Hay diferentes tecnologías: la llamada FTTH (fibra óptica hasta el hogar), el cable (introducido en principio por distribución de TV), el satélite y la RDSI (soportada por la red telefónica tradicional) entre otras. El modelo de desarrollo de la conectividad en cada país ha sido diferente y han dado lugar a distintas estructuras de mercado.

[126] Los motivos para preferir conexiones de banda ancha son el no tener la línea telefónica ocupada, la velocidad del acceso y la posibilidad de estar siempre conectado, así como el acceso a nuevos servicios relacionados con la fotografía, la descarga de música o vídeos. De menor manera, en el hogar, el equipo de conexión a Internet (módem/*router*) permite crear un entorno de red.

[127] Aunque su principal función es la transmisión de voz, como en el teléfono convencional, su rápido desarrollo ha incorporado otras funciones como cámara fotográfica, agenda, acceso a Internet, reproducción de vídeo e incluso GPS y reproductor mp3.

[128] Estas redes se pueden implementar por medio de cables y también sin hilos; es común que se disponga de redes sin hilos Wi-Fi .Véase Euribaromettres, (2009).

Las terminales son otro aspecto fundamental en las TIC pues actúan como punto de acceso de los ciudadanos a la sociedad de la información y son uno de los elementos que más han evolucionado: permiten aprovechar la digitalización de la información y la creciente disponibilidad de infraestructuras por intercambio de esta información digital.[129] Las novedades que hacen referencia a la capacidad y a la miniaturización de los dispositivos de almacenaje han permitido la creación de un conjunto de nuevos dispositivos portátiles que administran contenidos multimedia, como lo fueron los reproductores portátiles de MP3 o de video. (Maturana, 2008).

Con respecto a la computadora personal, según datos del dominio público, desde 2008 el número de PCs superó los mil millones en el mundo, encontrándose más del 60% en Estados Unidos, Europa y Japón. Actualmente, es la puerta de entrada más habitual a Internet y el navegador es la aplicación desde donde se accede a los servicios de la sociedad de la información y es la principal plataforma para las actividades informáticas.[130] Entre los principales servicios podemos mencionar el correo electrónico. La búsqueda de información, banca online, audio y música, el comercio electrónico, administración gubernamental, educación y entretenimiento**.** (Sarle y Rosas, 2005).

En los últimos años ha proliferado un conjunto de productos y formas de trabajo en la red, que se conocen bajo el concepto de Web 2.0. Son servicios donde un proveedor proporciona el soporte técnico, la plataforma sobre la que los usuarios auto-configuran el servicio. También han proliferado los *blogs* (bitácoras) donde en la web se recogen textos o artículos de uno o varios autores ordenados cronológicamente y escritos en un estilo personal e informal. Asimismo, las comunidades virtuales (redes sociales) que permiten a los usuarios crear perfiles y

[129] "Equipamientos en los hogares", 2009.

[130] La función tradicional de un navegador era la de presentar información almacenada en servidores. Con el tiempo, se fueron incorporando capacidades cada vez más complejas. Google entró en el mercado de los navegadores con el lanzamiento de Chrome. Su principal diferencia respecto a los navegadores tradicionales es que su estructura interna se parece más a un sistema operativo que ejecuta aplicaciones web que a un navegador web clásico.

listas de *amigos* como *MySpace, Facebook, Linkedin*. La globalización de las TIC permite un acceso continuo e ininterrumpido desde cualquier lugar del planeta, a un conjunto de recursos (datos, potencia informática), lo que implica también efectos en términos de seguridad y de ética.

Después de este esbozo técnico de los principales elementos de las TIC, basado sobre todo en referencias obtenidas en forma digital, concluimos este capítulo explicando que ha sido deliberado omitir el análisis del efecto sociológico de las mismas y su importancia histórica y científica en la sociedad actual pues además de que ya académicos como Mattelart, Martín Serrano, Karam y Castells lo han tratado con amplitud, ese sería tema de otra investigación.

Este trabajo requiere un abordaje descriptivo con una mirada crítica desde las ciencias sociales de un tema que hoy está ineludiblemente ligado tanto a nuestras actividades cotidianas como a aquellas relacionadas con la academia y el entorno profesional y que en muchos casos nos ha tomado por sorpresa. Aquí vale la pena retomar nuevamente el libro de Alva de la Selva (2015) pues analiza el tema desde un abordaje multidisciplinario e integral. Comienza con el contexto económico-político de las telecomunicaciones, las TIC y la sociedad de la información y el conocimiento, sin olvidar los contextos tecnológico, social y cultural. Parte de que sus objetos de estudio son conceptos dinámicos y los caracteriza desde sus propiedades básicas como la digitalización, la interactividad, la instantaneidad, la interconexión, la flexibilización y la innovación. En nuestro caso, retomamos esa valiosa investigación para centrarnos en el capítulo V de esta investigación en la historia de la criptografía computacional y con ello acercarnos cada vez más a las aportaciones de Turing y Shannon a su desarrollo.

Capítulo V
La criptografía computacional como forma de comunicación secreta en tiempos de guerra

En este capítulo ubicamos el papel de la criptografía computacional como una forma de comunicación secreta en la Segunda Guerra Mundial, a través de las herramientas de la hermenéutica profunda de John B. Thompson, planteadas en capítulos anteriores. Aunque éste es un capítulo en algunas de sus partes descriptivo y altamente técnico, se analizan, interpretan y reinterpretan los hechos a partir de su contexto sociohistórico y científico, con énfasis en el criptoanálisis y sus protagonistas (entre ellos, A. Turing y C. Shannon). Como otra de nuestras categorías generales, comenzamos con la definición de comunicación secreta y seguimos con la criptografía y el arte de ocultar y descifrar mensajes, así como con las tres etapas del criptoanálisis, la criptografía en las guerras mundiales y la diferencia entre criptografía simétrica y asimétrica.

V.1. Comunicación secreta

Para los fines de este trabajo de investigación, proponemos al *secreto* como un fenómeno comunicativo y una práctica social; como una acción comunicativa, en el sentido que lo hace Habermas (2015) que a la vez afecta a la comunicación. En palabras del académico F. J. Gallego Dueñas (2001), como una forma de relacionarnos los humanos… "una práctica social en la que un actor o actores, en una determinada situación, evitan, limitan o modifican la comunicación de algo (acción, pensamiento, sentimiento) a otro actor o actores, durante cierto tiempo, haciendo uso de ciertas tácticas, es decir, suponiendo un esfuerzo. Y no sólo cuando lo compartimos sino en todo momento, guardándolo y desvelándolo". También, en nuestro caso, cómo las condiciones de la acción comunicativa se ven afectadas por la existencia del secreto pues –sostiene el mismo Gallego Dueñas– "Aunque su apariencia es la de no divulgación, el funcionamiento del secreto en la vida social es esencialmente comunicativo.

Aquí partimos del supuesto de que un secreto trata sobre información relevante; no específicamente de una cualidad de la información sino del modo en el que esa información se transmite. Por eso hablamos de **plusvalía simbólica,** ya que no sólo ocultamos cosas que consideramos valiosas, sino que se otorga valor adicional a aquellas cosas que se convierten en secreto.[131]

Siguiendo con Gallego Dueñas (2001), retomamos una útil relación de los elementos del lenguaje del secreto y que podrían aplicarse a la criptografía:

Contexto

Emisor (anonimato) Mensaje **Receptor**
(silencio)

Canal (aislamiento)
Código (criptografía)
Referente (secreto convencional)

Partimos, entonces, de que la criptografía consiste precisamente en un lenguaje secreto en virtud de que se transmite a través de un medio y se oculta su significado original. De los métodos existentes, el más común es el cifrado, técnica que " …enmascara las referencias originales de la lengua por un método de conversión de un algoritmo que permita el proceso inverso o descifrado". El uso de esta técnica permite un intercambio de mensajes que sólo puedan ser leídos por los destinatarios que poseen la clave, un receptor autorizado. El algoritmo puede basarse en un código para el que resulta indispensable un *libro de códigos* (Gallego Dueñas, 2001).

[131] Véanse también los trabajos antropológicos de Bellman (1981) sobre la importancia del lenguaje en el secreto y como método para manejar información oculta. También lo que denomina idioma del secreto, así como la pragmática, que ponen en relieve las diferentes maneras de comunicar algo que sea secreto: comunicar sólo una parte, totalmente, dependiendo de quién lo escuche y quien lo enuncie, dependiendo del derecho a hablar y a entender. Edwin Black (1992) tiene, asimismo, trabajos interesantes sobre el secreto y su revelación.

De esa manera, "A través de la criptografía, no sólo se oculta el mensaje, sino también se oculta la cifra, la clave de su entendimiento. Una de las técnicas más importantes conceptualmente es el *secret sharing,* método mediante el cual se distribuye un mensaje entre un grupo de participantes, cada uno de los cuales comparte una parte". (Gómez, 2010 y Cascudo, 2010). En este esquema hay un emisor (*delaer)* y n actores (*players*). Así el transmisor envía el mensaje cifrado (el secreto) y envía la cifra en secreto. (Gallego Dueñas, 2001). Y seguimos con este autor pues estamos de acuerdo en que "El secreto ocupa, [o debería ocupar] un lugar en la teoría de la comunicación. El secreto nos ofrece un laboratorio doble de análisis: no sólo la semántica del contenido, sino también la pragmática y las situaciones que conforman la burbuja atmosférica del compartir un secreto". En este contexto, "La pragmática estudia la diferencia entre lo que el lenguaje codifica y lo que el lenguaje transmite, reflejando a su vez las relaciones sociales implicadas. La clave está entre la intención *comunicativa y la intención informativa*".[132]

Al referirnos al arte de ocultar (cifrar) y descifrar mensajes, necesariamente debemos tocar las tres etapas del criptoanálisis –manual o mecánico, electromecánico y electrónico o digital–, la evolución de la criptografía, con énfasis en las dos guerras mundiales, la criptografía simétrica (o de clave secreta) y asimétrica (de clave pública), el criptoanálisis moderno y la inclusión de Alan Turing y de Claude Shannon en nuestra área de estudio.

V.2. El arte de ocultar y descifrar mensajes

La criptografía surgió hace miles de años, cuando se comprendió que la información era un elemento que podría ser de gran utilidad para el control y el poder, por lo que ha encontrado múltiples aplicaciones prácticas en los campos militar, político y económico. El término criptografía proviene de las palabras latinas, *cripto* ocultar y *graphos* escritura y significa "arte de ocultar mensajes".

[132] Las cursivas son nuestras. Véanse Gallego (2001), y los debates de Sperber, Wilson y Grice, publicados en 2004.

La historia de la criptografía comenzó hace aproximadamente 4000 años, por el 1900 a. C. con un escrito de 20 columnas con 222 inscripciones sobre la tumba egipcia de un noble llamado Khnumhotep II, cerca del río Nilo, donde se encontraron inscritos jeroglíficos distintos a los símbolos usuales de la época. Se asumió, entonces, que de esta manera el verdadero significado del escrito permanecía en secreto. Se supone que la técnica usada en estos códigos fue de sustitución simple, es decir cada símbolo del mensaje original se sustituyó por otro símbolo, y sólo la persona que sabía los reemplazos correctos, podía descifrar el mensaje (Kahn, 1967 y Deavours, 1985).

Uno de los mensajes cifrados más antiguos es la fórmula para hacer esmalte de cerámica en Mesopotamia, mediante la sustitución simple, utilizada en el año 1500 a. de C. El primer algoritmo de cifrado (o conjunto de operaciones sistemáticas que permiten hacer un cálculo y hallar la solución de un tipo de problemas) se ubica en 590 a. C. Es cifrado por que utiliza un algoritmo con cierta clave incomprensible para quien no la conozca. Uno de los primeros métodos criptográficos esquemáticos es el llamado *atbash* y consistía en cifrar mensajes usando el alfabeto en reversa: de la Z a la A.

Por el año 487, los espartanos de Grecia crearon la primera máquina de cifrado, (conocida más tarde como *skytale*), que consistía en una pieza de madera y una cinta de cuero que era enrollada en la madera, donde se escribía el mensaje secreto. El mensaje se transmitía sólo por la cinta usada como cinturón y para descifrarlo se debía conocer el diámetro de la madera. Otra técnica de cifrado griega fue la tabla, o *polybius*, en la que se asociaba a cada letra un par de números enteros; fue pensada como medio de comunicación telegráfica. (Kahn 1967 y Deavours 1985).

Antes de nuestra era (100-44 a. de C.), al emperador romano Julio César se le atribuye el uso del método de cifrado más conocido de la Antigüedad. Consistía en

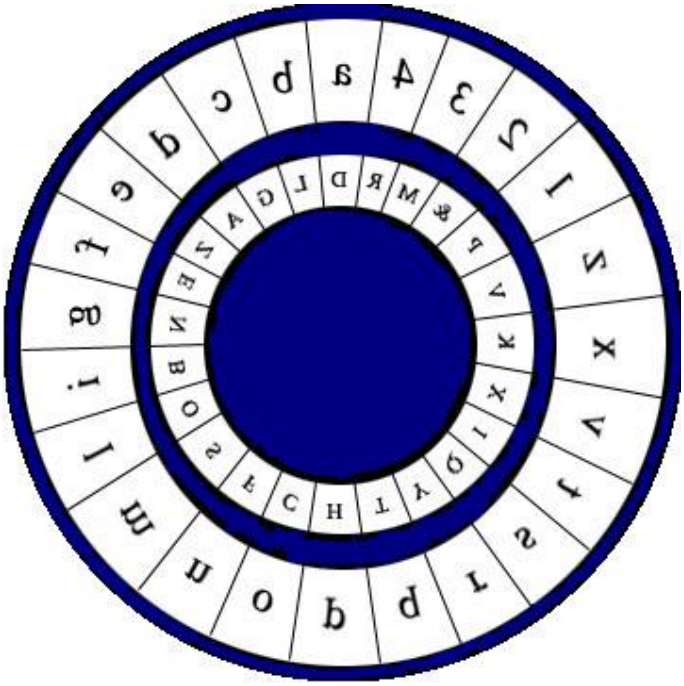
aplicar una función lineal.[133] Como ejemplo, para explicarla, se suele usar la palabra HOLA, que se cifra como ELIX[134] y es uno de los textos más sencillos de un sistema criptográfico que usa una *transposición* (permuta los elementos del mismo conjunto). Aunque en los primeros años de nuestra era existieron distintos sistemas criptográficos, la mayoría de ellos se basaban en sustituciones y transposiciones como la siguiente:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

En 1466, Leon Battista Albertini inventó el que se considera el primer disco para cifrar**:** un cifrador compuesto en realidad por dos discos, uno exterior y otro interior. El exterior contenía el alfabeto latín; el inferior, su *sustitución*. Fue el primero en usar un disco y una posición como clave de cifrado, ideas que formarán parte de las máquinas de cifrado del siglo XX. (Kahn y Friedman,1967: 844-851).

[133]Que sólo para los interesados y entendidos, se expresa así: La f(x)=x+b, módulo 26 con b=3.

[134] Estos ejemplos se usan frecuentemente en libros de criptografía general. Para los entendidos, el sistema de Julio César puede ser extendido a la función $f(x)=ax+b \bmod n$, con mcd(a, n)=1.



El primer método compuesto para cifrar se adjudica a Blaise de Vigenére, quien en 1523 inventó un famoso sistema de cifrado, que de algún modo generalizaba el de Julio César. Usando la función lineal de cifrado $f(x)=x+b \bmod n$, donde x es el mensaje a cifrar y b la clave de cifrado.[135] Para efectuar este cifrado se usaba la siguiente tabla:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

[135] Este ejemplo es utilizado por diversos historiadores de la criptografía como Khan (1967), 1996), Martín Reina (2003, 2009) y Ángel, José de Jesús (s.f.) en su "Criptografía para principiantes".

Las letras de la primera fila corresponden a las letras del mensaje original, las letras de la primera columna, a las letras de la clave. Se toma cada letra del mensaje original (i), y se elige la letra correspondiente de la clave en la primera columna (j), entonces la letra que está en la intersección (ij) es la letra cifrada correspondiente.[136] Entonces el mensaje cifrado es:

H	→	H+E	=	L
O	→	O+S	=	G
L	→	L+T	=	E
A	→	A+A	=	A
M	→	M+L	=	X
U	→	U+L	=	F
N	→	N+A	=	N
D	→	D+V	=	Y
O	→	O+E	=	S

Durante los siglos posteriores se afinaron los sistemas criptográficos. Entre 1790 y 1800, por ejemplo, Thomas Jefferson, expresidente de los Estados Unidos, inventó el primer dispositivo manual-mecánico para cifrar: consistía en un conjunto de discos que giraban alrededor de un eje en los que se grababa el alfabeto de manera aleatoria. Para cifrar un mensaje, se colocaban los discos en un orden establecido (la llave), se alineaba el mensaje y tomaba como mensaje cifrado cualquiera de las otras letras alineadas. Etienne Bazeries mejoró ese sistema en 1901, que posteriormente sería básico para los dispositivos usados por el ejército y la marina estadounidenses en 1914, durante la Primera Guerra Mundial.[137]

[136] En términos de la fórmula queda como: $f(x_i)=x_i+b_i \bmod n$. Como ejemplo; para cifrar el mensaje "HOLA MUNDO" (los x_i), se elige una palabra clave de la misma longitud que el mensaje original, por ejemplo "ESTA LLAVE" (cada letra corresponde a un b_i). Véase Kahn y Friedman (1967).

[137] Entre otros, véase a Kahn (1967) y Deavours (1985).

Pero todavía en el siglo XIX, alrededor del año 1880, un noble francés, el Marqués de Viaris, ideó una máquina para cifrar mensajes, que sería básica para los dispositivos criptográficos del siguiente siglo. La segunda etapa de la criptografía ocurre entre 1910 y 1920 y corresponde a las máquinas cifradoras. Según varios registros historiográficos, la primera de ellas fue inventada por los holandeses Van Hengel y Spengler; en 1916, Arvid Gerhard Damm patentó en Holanda otra máquina; un año después, Edward Hebern inventó una que usaba un rotor y, en 1919, el también holandés, Hugo Koch patentó otra aún más compleja.

La máquina de cifrar más conocida ha sido la alemana Enigma, cuya primera versión se basó en la máquina de Arthur Scherbius, patentada en 1918. Posteriormente se derivaron otras, particularmente las Enigma, primero con tres discos y después con cinco discos, a las que nos referimos ampliamente en el capítulo VI de este trabajo.

Cabe resaltar otras máquinas de cifrar muy similares a Enigma como Sigaba, usada por el ejército estadounidense durante la Segunda Guerra Mundial y Typex, y Combined Cipher Machine (CCM), del ejército Inglés y los aliados durante la misma conflagración mundial. Las últimas máquinas de cifrar, más sofisticadas que Enigma, creadas en la década de los años cincuenta, fueron XL-7, HX-63. OMI, M-125, OH-4605, Gretacoder 805, HC-520, KL-51, MK-85C. En los años sesentas del siglo XX, algunas ya incluían circuitos electrónicos y programas de computadora.[138]

Las máquinas de cifrado fueron desapareciendo entre los años sesenta y setenta. Se da entonces el comienzo de la época de oro de la criptografía con la invención de la criptografía de clave pública en 1974, aspecto al que nos referimos con más detalle más adelante en este capítulo.

[138] Tanto Martín Reina, Daniel (2003), (2009): como Kahn (1967) y Deavours (1985) explican esta parte de la historia de la criptografía con distintos niveles de complejidad.

Por su naturaleza, la criptografía había sido utilizada principalmente en periodos de guerra, o en medios relacionados con la seguridad nacional de muchos países. En la actualidad se usa también y ampliamente en diversas aplicaciones relacionadas con las tecnologías de la información y la comunicación como Internet, teléfono, radio, televisión, comunicación satelital y en los ámbitos educativo, económico, bancario y comercial.

V.3. Los elementos de la criptografía

El objetivo principal de la criptografía es enviar un mensaje de manera oculta, llamado *cifrado* o *encriptado*, y cuyo contenido sólo pueda "descifrar" el receptor que posea una llave o clave secreta determinada. Si los elementos básicos de cualquier comunicación son emisor, receptor, mensaje y canal de transmisión del mensaje, los elementos básicos que intervienen en la criptografía son *mensaje original*, *método de cifrado*, *llave de cifrado*, *mensaje cifrado*, *método de descifrado*, *llave de descifrado* y *mensaje descifrado*. La criptografía, más el criptoanálisis (arte de romper códigos y cifrados) da por resultado la criptología.

En criptografía se supone siempre la existencia de un *agente* que tiene la capacidad de interceptar el mensaje enviado y quiere saber su contenido. Así, el objetivo principal de la criptografía es evitar que el interceptor conozca el contenido del mensaje. (Martín Reina, *2009).*

La escritura secreta que usaban, por ejemplo, los Césares romanos al sustituir cada letra por otra situada unas posiciones antes o después, se le denomina criptografía *de sustitución* pues cada letra del mensaje inicial se sustituye por otra. En cambio, en otros cifrados, como los *de trasposición*, las letras del mensaje sólo cambian de lugar, generándose un anagrama. (Un ejemplo de trasposición es el del escítalo espartano, al parecer, el primer aparato criptográfico militar de la historia).[139]

[139] El escítalo era un bastón, del que se tenían dos ejemplares idénticos. El emisor enrollaba una tira de cuero alrededor del bastón y escribía longitudinalmente sobre el mismo el mensaje que quería transmitir. Entonces se retiraba la cinta, quedando un mensaje incomprensible –el mensaje cifrado- y se enviaba al

V.3.1. El criptoanálisis

El criptoanálisis es la disciplina dedicada a obtener información de una transmisión interceptada sin el conocimiento de la clave. Según registros históricos, el primero en descifrar un mensaje sin conocer la clave fue el científico árabe del siglo IX Al Kindi quien desarrolló una técnica para conocer los códigos de sustitución monoalfabéticos (como el de Julio César, al que a cada letra le corresponde sólo una letra distinta) y realizó análisis de frecuencias, que consiste en estudiar la frecuencia con que cada letra del alfabeto aparece en un texto normal en determinado idioma.[140]

Con el nacimiento del criptoanálisis y el descubrimiento de su utilidad en el espionaje y la guerra, tuvieron lugar cruentas batallas entre creadores de cifras y descifradores. Durante el Renacimiento la criptografía se convirtió en una herramienta diplomática y algunas cortes europeas llegaron a crear los primeros sitios dedicados exclusivamente al criptoanálisis. En esa época se desarrolló la llamada criptografía de sustitución polialfabética, que consistía en una mezcla de sustituciones monoalfabéticas. De esta manera resultaba que una misma letra del texto original podía acabar representada por diferentes letras en el texto cifrado, siendo así inexpugnable al análisis de frecuencias. El método más conocido es el "tablero de Vigenère", tabla formada por el alfabeto llano seguido por 26 alfabetos cifrados, consiguiéndose cada uno de ellos comenzando en la siguiente letra del anterior.[141]

---

destinatario, que disponía de una copia del escítalo. Al colocar la cinta sobre el bastón, se recuperaba el mensaje, si se conocía el diámetro exacto del escítalo. Así, se podían transmitir órdenes en las campañas militares. (Kahn, 1967).

[140] En castellano la más frecuente es la "a"; en inglés, la "e". Procediendo con lógica y aplicando algún truco (como centrarse en las palabras de una sola letra o sílaba, o en las vocales) se puede descifrar el código.

[141] Para cifrar un mensaje con el tablero de Vigenère y la clave HIELO (por ejemplo), lo primero es repetir la clave sobre el texto llano tantas veces como sea necesario, hasta que cada letra del mensaje quede asociada con una letra de la clave. Para cifrar cada letra, se busca la línea del tablero de Vigenère identificada por la letra de la clave (la línea tal que la A se encripta como la letra de la clave), y en esa línea buscamos la cifra correspondiente a la letra del texto llano. Aunque era efectivo por su dificultad, la urgencia en las comunicaciones militares la hicieron obsoleta. Véase Singh (2000).

La invención del telégrafo, a principios del siglo XIX, revolucionó las comunicaciones en el mundo pues por primera vez una noticia se pudo difundir al momento de producirse. La información fue adquiriendo valor y la criptografía comenzó a desarrollarse como una disciplina. La invención de la radio a finales del siglo XIX y el estallido de la Primera Guerra Mundial intensificaron la necesidad de una encriptación cada vez más segura. Las distintas potencias intentaron usar la facilidad de comunicación de la radio pero se sentían vulnerables debido a la facilidad con que sus mensajes podían ser interceptados. Se trabajaba arduamente para encontrar la cifra definitiva aunque al final, los mejores criptoanalistas las descifraban. (Martín Reina, 2003).

V.3.2. Tres etapas del criptoanálisis

La evolución de la criptografía ha ido de la mano de la evolución del criptoanálisis. Su importancia radica en que el descubrimiento y aplicación del análisis de frecuencias a la lectura de las comunicaciones cifradas ha cambiado en no pocas ocasiones el curso de la historia. Quizás las más destacadas sean el desciframiento del ya mencionado telegrama Zimmermann, que aceleró la entrada de Estados Unidos a la Primera Guerra Mundial, y la lectura, por parte de los Aliados, de los mensajes cifrados de la Alemania nazi, para haber acortado la Segunda Guerra Mundial varios años y que seguimos tratando más adelante. (Friedman, 1967 y Simmons, 1967).

La criptografía es hoy la disciplina que estudia los problemas de seguridad en la transmisión de la información por medio de un canal que se supone siempre inseguro. Los principales problem*as* que existen en la seguridad de la transmisión de la información son la *confidencialidad,* la *autenticidad*, la *integridad*, la *disponibilidad* y el *no rechazo.* (Ángel, s.f.).

La información es *confidencial,* si solo las personas autorizadas tienen acceso al contenido de la información; es *integra*, sí existe un método con el cual se puede verificar si la información transmitida ha sido alterada o borrada (pues no es

posible impedir que sea interceptada, alterada o eliminada). La comunicación (emisor o receptor) puede verificar la autenticidad del otro lado, si existe un método de *verificación* que determina que el otro lado es realmente quien dice ser.[142]

Como hemos apuntado anteriormente, la historia de la criptografía se puede dividir en tres etapas, 1) cuando los dispositivos criptográficos eran *manuales o mecánicos*. 2) cuando los dispositivos eran *electromecánicos* y 3) cuando los dispositivos son *electrónicos y digitales*.

La primera etapa se caracteriza por usar medios de cifrado que operaban manualmente o con algún dispositivo mecánico, es decir, desde los orígenes de la sociedad hasta los años 1900. A este tipo de criptografía se le conoce también como *criptografía clásica*. La segunda etapa corresponde a los dispositivos electromecánicos que datan de los años veinte del siglo pasado y cuyo dispositivo más reconocido es la máquina alemana Enigma. La tercera etapa ocurre a la par de la era de las computadoras, por los años sesenta y setenta del siglo XX. Esta etapa de la criptografía comienza con el algoritmo DES (*Data Encryption Standard*) y sigue hasta nuestros días, con avances tan sorprendentes como los relacionados con la criptografía cuántica. (Martín Reina, 2003).

[142] Se dice que un acto no puede ser *rechazado* por el lado A de la comunicación, si existe un método que le comprueba al otro lado, el lado B, que ese acto lo realizó realmente. La información es *disponible* si está accesible a toda entidad que la requiera, ya sea una persona o un dispositivo y que cumpla los objetivos que la misma entidad le provee. Véase D. Icove, *et al*., (1995). Entre algunas aplicaciones de la criptografía, en Internet, el protocolo se llama SSL (*Secure Sockets Layer*); en teléfonos celulares, GSM (*Global System for Mobile communications*); servidores a largas distancias de manera segura, VPN (*Virtual Private Network*); computadoras manera segura, con IPsec (*Internet Protocol Secure*); teléfono por Internet de manera segura, VoIP (*Voice over Internet Protocol*) e-mail de manera segura, S-MIME (*Secure / Multipurpose Internet Mail Extensions*); usar un PDA (Personal Digital Assistant) de manera segura, WTLS (*Wireless Transport Layer Security*); conectar una portátil a internet de manera segura, con el protocolo WEP (*Wired Equivalent Privacy*); videos, televisión por Internet con BitTorrent; etiquetas electrónicas, *Radio Frequency Identification* (RFID), con TI-RFid; comunicación satelital con el protocolo GMPCS (*Global Mobile Personal Communications by Satellite*); "Facturas Electrónicas", con la firma digital. Comprar, vender o mandar dinero por Internet con Paypal; cajeros automáticos ATM (*Automatic Teller Machine*); En tarjetas inteligentes electrónicas (*Smart Cards*). Véase Koblitz (1994).

V.3.3. Criptografía en las guerras mundiales

Dos de los hechos más importantes de la historia mundial del siglo XX estuvieron relacionados con la criptografía. Como ya lo mencionamos en el capítulo II de esta investigación, el primero de ellos ocurrió en México durante la Primera Guerra Mundial; el otro, en la Segunda Guerra Mundial y entre sus protagonistas se encuentran Alan Turing y Claude Shannon.

Al primer hecho se le conoce como *Telegrama Zimmermann* y marcó la participación de Estados Unidos en la Primera Guerra Mundial. En dicho telegrama, Alemania proponía a México unirse en contra de Estados Unidos para formar una alianza con Japón y, a cambio, al derrotar a los estadounidenses, regresar a México los territorios perdidos de Texas, Arizona y Nuevo México. La Primera Guerra Mundial llevaba casi tres años y Estados Unidos permanecía neutral antes de descifrar ese documento.[143] El 29 de Marzo, el propio Zimmermann admitió la existencia del telegrama y una semana después, el 6 de Abril de 1917, Estados Unidos entró a la Primera Guerra Mundial y el 14 de Abril, el presidente mexicano Venustiano Carranza declinó oficialmente la oferta de Alemania. (Kahn, 1967, Friedman, 1967 y Martín Reina, 2003).

Como hemos dicho, en la Segunda Guerra Mundial la criptografía fue muy utilizada y de hecho fue determinante en su desarrollo y eventual término. En ello profundizamos en el capítulo VI.

La tercera etapa de la historia de la criptografía inició de manera paralela con el uso masivo de las computadoras. Existen diversos hechos importantes en esta

[143] El 16 de enero de 1917, Zimmermann envió un telegrama a Heinrich von Eckardt, embajador Alemán en México,. El telegrama se envió, al menos por dos vías diferentes: un cable a Washington y por una embarcación sueca. El primero fue cifrado con un "*book code*" llamado 0075, pero como aparentemente ese código era desconocido por la embajada alemana en México, fue reenviado cifrándolo con un código más simple denominado 13040, que consistía en una lista de alrededor de 75 mil códigos con 25 mil palabras a codificar. El código 13040 era ya muy conocido por el grupo de criptoanalistas ingleses llamado "Room 40". El 4 de Febrero de 1917, Estados Unidos rompió relaciones con Alemania. Unos días después, el 23 de Febrero, el telegrama descifrado llegó a Estados Unidos proveniente de Inglaterra y el 1o. de Marzo la prensa estadounidense publicó la noticia del telegrama.

etapa[144] pero sólo mencionamos algunos de ellos pues no son el objetivo central de esta investigación.

V.3.4. Criptografía simétrica o de clave secreta y asimétrica o de clave pública

La criptografía simétrica es el sistema de cifrado más antiguo. Consiste en que tanto el emisor como el receptor encriptan y desencriptan la información con una misma clave secreta (*k),* que ambos comparten. Es el conjunto de algoritmos que funciona con una sola llave o clave, que tienen ambos lados de la comunicación y que debe de permanecer secreta. Casi toda la criptografía usada antes de 1974 era simétrica. De la criptografía simétrica deriva uno de los principales problemas de la criptografía, que es el intercambio de las claves secretas (o claves simétricas). El funcionamiento es muy sencillo: el emisor cifra el mensaje con la clave *k* y se lo envía al receptor. Este último, que conoce dicha clave, la utiliza para desencriptar la información.[145]

Las criptografías de sustitución y trasposición pertenecen a la criptografía simétrica de clave secreta; el problema era la distribución de las claves, aspecto que se resolvió plenamente hasta el último cuarto del siglo XX. (Martín Reina, 2003). El sistema criptográfico de clave secreta más utilizado es el DES de IBM y fue adoptado por las oficinas gubernamentales estadounidenses para proteger sus datos desde 1977. Este sistema de cifrado es altamente eficiente dado que los algoritmos utilizados son muy rápidos al poder aplicarse tanto en *hardware* como en *software*.

[144] En 1976 Diffie-Hellman creó un esquema de intercambio de claves basado en el *Problema del Logaritmo Discreto*, dando lugar a la criptografía de clave pública. En 1977 Ron Rivest, Adi Shamir y Len Adleman crearon el sistema RSA para el intercambio de claves y firma digital. En 1985, N. Koblitz y V. Miller introdujeron las curvas elípticas en la criptografía de clave pública; su mayor aporte fue la reducción de la longitud de las claves de 1024 bits a 160. En 1989, N. Koblitz propuso utilizar las curvas hiperelípticas en el uso de la criptografía de clave pública. En 2001, Boneh y Franklin crearon la criptografía bilineal, poniendo en práctica sistemas de cifrado basados en la identidad, es decir, que la clave pública puede ser cualquier cadena de caracteres.

[145] Para que el sistema sea *fuerte* contra ataques de tipo criptoanálisis, la clave *k* debe ser mayor de 40 bits, lo cual choca con las restricciones de exportación de tecnología criptográfica del gobierno estadunidense, que marca los 40 bits como límite de clave para programas que utilicen este tipo de tecnología. DES, IDEA y RC5 son algoritmos típicos que utilizan cifrado simétrico.

Actualmente la criptografía simétrica se usa para cifrar grandes cantidades de información de la manera más rápida. La clave secreta del algoritmo simétrico se intercambia previamente con un algoritmo asimétrico, y se usa un modo de operación en función del objetivo del cifrado. Los algoritmos de cifrado se dividen en ***Cifradores de bloque***[146] (*Block Ciphers*) y ***Cifradores de flujo*** (*Stream Ciphers*), los primeros cifran por bloques de *bits* los segundos cifran *byte* por *byte* o *bit* por *bit*. [147]

El mayor inconveniente de la criptografía simétrica es que esta clave *k*, al ser compartida, debe ser comunicada de forma segura entre las dos partes de la comunicación (por teléfono, correo certificado, etc.), previamente a ésta. Si el secreto fuera enviado por un canal inseguro, como Internet, cualquiera podría interceptarla y comprometer todo el sistema. También hay que tener en cuenta la frecuencia con la que esta clave debe ser renovada para evitar que sea develada. También debe tomarse en cuenta el manejo de estas claves[148]. Ambos problemas se resuelven con la llegada de los criptosistemas de clave pública o asimétrica.

Por su parte, la criptografía de clave pública o asimétrica, inventada por Diffie-Hellman en 1976, resuelve el problema del intercambio de claves simétricas. En la actualidad, casi siempre se usa primero la criptografía de clave pública para el intercambio de la clave simétrica y luego la criptografía simétrica para el cifrado de

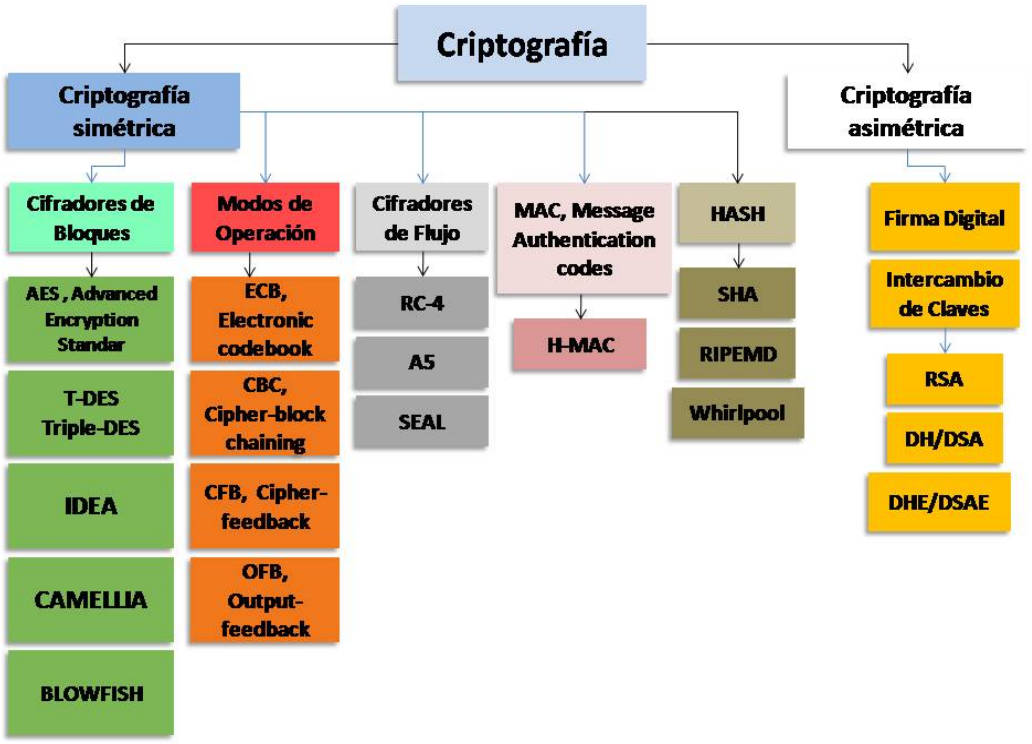
[146] Algunos sistemas conocidos del cifrador de bloque son TDES, RC5, AES. Los cifradores de flujo más conocidos son RC4, SEAL, WAKE.

[147] Descripción del estándar de cifrado simétrico AES (*Advanced Encryption Standard*). Para cifrar cantidades pequeñas de información se usa el modo de operación ECB; para cifrar cantidades grandes, el CBC. El modo de operación CFB convierte a un cifrador de bloques en uno de flujo. El modo de operación OFB, además de convertir un cifrador de bloques en uno de flujo evita el error de propagación. Otros algoritmos auxiliares que son usados como algoritmos simétricos son los MAC, algoritmos que muestran a una de las partes que el mensaje recibido tiene el origen de alguien que posee una clave simétrica específica.

[148] En una red de n usuarios, cada pareja necesita tener su clave secreta particular, lo que hace un total de n(n-1)/2 claves para esa red (es decir, combinaciones de n usuarios tomadas de 2 en 2. Eso supone unas cinco mil claves en una red de sólo cien usuarios, medio millón en una de mil, y varios billones en sistemas de telefonía convencional de un país. Es económicamente inaceptable que se puedan distribuir todas estas claves por anticipado, e indeseable el tener que posponer las comunicaciones seguras mientras las claves están siendo trasladadas de una a otra parte.

toda la sesión. Los sistemas de clave pública más usados en la actualidad son los esquemas de intercambio de claves y los esquemas de firma digital.[149]

El siguiente organigrama, reproducido ampliamente en varios libros y en algunas páginas de Internet, entre las que se encuentra el blog "Criptografía para principiantes" de Ángel Ángel, José de Jesús (s.f.) muestra las ramas más generales de la criptografía desde el punto de vista de los algoritmos que la componen:



[149] Los sistemas de clave pública más usados son el sistema RSA, basado en el problema de la factorización entera; DH/DSA, en el problema del logaritmo discreto y DHE/DSAE, basado en el problema del logaritmo discreto elíptico. Un protocolo de seguridad es la parte visible de una aplicación; es el conjunto de programas y actividades programadas que cumplen con un objetivo específico y que usan esquemas de seguridad criptográfica. El ejemplo más común es SSL (*Secure Sockets Layer*), integrado en el *Browser* de Netscape y aparece cuando el candado de la barra de herramientas se cierra y si la dirección de Internet cambia de http a https. Véase Ángel (s.f.), Kahn (1967, 1996) y Deavours (1985).

Como se mencionó al inicio de este capítulo, el criptoanálisis es la disciplina que se dedica a analizar los sistemas criptográficos para inferir una clave, parte de una clave, mensajes descifrados, etc. a partir de las *debilidades* de un sistema.[150] En páginas anteriores explicamos la importancia de la criptografía como un pasatiempo, un arte o una estrategia de comunicación secreta en tiempos de guerra.

En el siguiente capítulo nos centramos en las aportaciones criptográficas de Turing y la publicación en 1949 de la *Teoría de la Criptografía* de Shannon, la cual fue aplicada por el NBS (*National Bureau of Standars*) de Estados Unidos para desarrollar el sistema criptográfico DES (*Data Encryption Standard*). Veremos cómo la criptografía salió a la luz pública y empezó a ser considerada una ciencia aplicada, debido a su relación con otras, como la estadística, la teoría de números, la teoría de la información y la teoría de la complejidad computacional.

V.4 Dos máquinas para la guerra

En la criptografía, la máquina Enigma divide la criptografía clásica y la moderna, entre la de antes y la de después de la existencia de las computadoras; cifrados con máquinas que utilizan la corriente eléctrica pero con principios de funcionamiento mecánicos. [151]

Su existencia produjo importantes avances tecnológicos. En 1923 el ingeniero alemán Arthur Scherbius patentó Enigma, máquina diseñada para facilitar las comunicaciones seguras. Su nombre se convirtió en sinónimo de secreto militar y evoca imágenes de espionaje y laboratorios ocultos pero, con toda su sofisticación, es, en esencia, una versión mejorada del disco de Alberti.

[150] En lenguaje coloquial se dice que se ha *descifrado* el sistema criptográfico cuando se ha descubierto una *debilidad* considerable en el mismo.

[151] Véase Martínez Navarro, Germán ( ) y http://www.worldlingo.com/ma/enwiki/es/Enigma_machine, http://en.wikipedia.org/wiki/Enigma_machine, Gómez, Joan (2010). Para Typex, véase http://www.worldlingo.com/ma/enwiki/es/Typex y http://en.wikipedia.org/wiki/Typex.

La máquina Enigma se parecía a una máquina de escribir. Constaba de un teclado y un tablero luminoso de 26 letras; tres rotores o modificadores, que podían permutar sus posiciones, montados sobre ejes, con 26 posiciones posibles, y un clavijero, para realizar un primer intercambio de letras en función del modo en que se dispusieran las clavijas.

El proceso físico de cifrado era relativamente sencillo. En primer lugar, el emisor disponía las clavijas y los rotores en una posición de salida especificada por el libro de claves que estuviera vigente en ese momento. A continuación, tecleaba la primera letra del mensaje llano y la máquina, de forma automática, generaba una letra alternativa que se mostraba en el tablero luminoso: la primera letra del mensaje cifrado.

Una vez completado ese proceso, el primer rotor rotaba en la siguiente de sus 26 posiciones posibles. La nueva posición del modificador conllevaba un nuevo cifrado de los caracteres, y el emisor introducía entonces la segunda letra, y así sucesivamente. Para descodificar el mensaje, bastaba con introducir los caracteres cifrados en otra máquina Enigma con los parámetros de salida iguales a los de la máquina con la que se había llevado a cabo la encriptación.

Con el rotor en la posición inicial, cada letra del mensaje original se sustituía por una distinta, excepto la A, que quedaba inalterada. Tras el cifrado de la primera letra, el rotor se desplazaba 1/3 de vuelta. En esta nueva posición, las letras eran sustituidas por otras distintas a las del primer cifrado. El proceso se completaba con la tercera letra, momento en el cual el rotor volvía a su posición inicial y la secuencia de cifrado volvía a repetirse.

Como ya se ha indicado, los modificadores de la Enigma estándar tenían 26 posiciones, una para cada letra del alfabeto. En consecuencia, un modificador era capaz de llevar a cabo 26 cifrados distintos. La posición inicial del modificador era, por tanto, la clave. Para aumentar el número de claves posibles, Enigma tenía en

un principio tres rotores, conectados de forma mecánica uno con otro. Así, cuando el primer rotor completaba una vuelta, el siguiente iniciaba otra, y así hasta completar las rotaciones completas de los tres rotores con millones de posibles cifrados. Además, el diseño de Enigma permitía intercambiar el orden de los rotores, aumentando todavía más el número de claves y disponía también de un clavijero situado entre el primero de ellos y el teclado. Ese clavijero permitía intercambiar entre sí pares de letras antes de su conexión con el rotor y añadía un número considerable de claves adicionales al cifrado. El diseño estándar de la máquina Enigma poseía seis cables, con los que se podían intercambiar hasta seis pares de letras y se podían cifrar un texto utilizando más de diez mil billones de combinaciones diferentes.

Typex (1937) fue una máquina similar, variante británica de Enigma. Poseía cinco rotores. Normalmente los dos primeros rotores permanecían inmóviles durante el cifrado, aunque podían ser movidos manualmente. Esos dos rotores adicionales proveían a Typex una seguridad adicional similar a la que las clavijas a Enigma. Algunos rotores de Typex se dividían en dos partes: el rotor y un *slug* (una especie de caja donde se tenía el cableado) insertado en una carcasa de metal. Cada una de estas carcasas podían tener diferentes muescas en su borde (5, 7 ó 9). Cada slug podía ser insertado en la carcasa de dos formas: normal y dándole la vuelta. Normalmente se tenían diez slugs, de los cuales se elegían cinco.

Las versiones de Typex tenían una serie de ventajas sobre la máquina Enigma: Enigma requería de dos operadores, uno para introducir el texto en la máquina y otro para copiar los caracteres ya criptografíados que se iluminaban en el panel, mientras que Typex necesitaba un único operario. Typex evitaba los errores producidos por el encargado de copiar a mano el texto cifrado o descifrado, ya que éste era impreso en una cinta de papel. A diferencia de Enigma, las Typex I estaban conectadas a teletipos, mientras que las Typex II lo estaban si querían. En Enigma los mensajes debían introducirse a mano en la máquina, encriptados por ésta, y una vez encriptados, transmitidos (por Morse). Cuando el mensaje

encriptado era recibido debía ser escrito nuevamente a mano en la máquina, desencriptado por ésta, y escrito a mano el resultado. Mientras que los mensajes en Typex eran impresos automáticamente y a encriptados y transmitidos inmediatamente por el hecho de estar conectadas a teleimpresoras. Esto dio una ventaja importante a los británicos.

Así como en este capítulo se ubicó el papel de la criptografía computacional como una forma de comunicación secreta en la Segunda Guerra Mundial a través de las principales herramientas de la hermenéutica profunda; se analizaron e interpretaron los hechos a partir de su contexto sociohistórico, con énfasis en el criptoanálisis y sus protagonistas y se tomó en cuenta el análisis discursivo de la propia hermenéutica en su momento diacrónico y sus elementos paradigmáticos, en el VI capítulo analizamos puntualmente las aportaciones de Turing y Shannon para el desarrollo de la computación, las TIC y la comunicación contemporánea pues sin ellos no hubiera sido posible el lenguaje binario, la computación como hoy la conocemos y sus aplicaciones; tampoco el desencriptar algunas de las máquinas alemanas y cambiar, simplemente, el curso de la historia.

Con respecto a los niveles de interpretación y reinterpretación acotados por Thompson, estamos convencidos de que en su momento (contexto sociohistórico) no se alcanzó a comprender la magnitud e importancia de lo que Turing y Shannon estaban haciendo. Hoy, a décadas de distancia, revaloramos (reinterpretamos) en su más justa dimensión las aportaciones de ambos y su crucial importancia no sólo para sus campos específicos de acción (en las matemáticas y la ingeniería) para terminar una guerra y salvar a millones de seres humanos de ambos bandos (aquí entran el nivel diacrónico y elementos paradigmáticos), sino también dentro de otros campos de acción en los que han sido ignorados: las ciencias sociales, las ciencias de la comunicación y las tecnologías de la información y la comunicación.

Capítulo VI

Aportaciones de Turing y de Shannon a la criptografía, a la comunicación secreta y a las TIC

Después de ubicar la teoría de la interpretación como estrategia metodológica de análisis, de visualizar con el modelo de análisis hermenéutico las categorías generales en dos mentes, un tiempo y dos espacios con respecto a la comunicación secreta y la criptografía computacional en las actuales TIC, en este capítulo entrelazamos las vidas y aportaciones de Turing y Shannon a las ciencias de la comunicación a través de la comunicación secreta y las TIC durante los primeros sesenta años del siglo XX en el mundo anglosajón tanto en Europa como en América. Terminamos esta investigación con el propósito de incorporarlos apropiadamente a nuestros proyectos de investigación y programas académicos y de ubicar cabalmente la comunicación secreta a nuestros planes de estudio.

VI.1. Turing y Shannon en la criptografía, en la comunicación secreta y en las TIC

En el artículo "Alan M. Turing y Claude E. Shannon: matemáticas para la informática", Llorenc Huget Rotger explica que junto al matemático húngaro John von Neumann (1903-1957), ambos figuran entre los pioneros de la informática pues "Turing y von Neumann pusieron las bases para el desarrollo del ordenador y Shannon las de las tecnologías de la información".[152]

Como matemáticos, Turing y Shannon habían trabajado (desde la lógica formal de Boole) en líneas complementarias sobre la ***decidibilidad***, en el sentido de determinar si se puede diseñar un procedimiento mecánico mediante el cual, partiendo de una proposición, y con un número finito de pasos, se pueda concluir

[152] Publicado en el diario español *El país*, en 2012 como parte de las celebraciones del Año Turing. Por otro lado, *von Neumann* es el catalizador de los trabajos de *Shannon* y *Turing,* que ambos habían realizado, previamente, en el Instituto de Estudios Avanzados de *Princeton*, y que ha llevado a consagrar la arquitectura de los ordenadores actuales como la arquitectura *von Neumann*, basada en programas almacenados en memoria, y desarrollada en los proyectos EDVAC y ENIAC, siendo éste considerado como el primer ordenador electrónico de propósito general.

si esta proposición es verdadera o falsa. Como indicamos en capítulos anteriores, en 1936 Turing presentó su trabajo "*On the Computable Numbers, with an Application to Entscheidungsproblem*" (decisión), demostrando la imposibilidad de ese proceso. En ese artículo, Turing reemplazó el lenguaje formal basado en la aritmética de Gödel por el concepto de máquina de calcular, constituyendo la base de lo que hoy conocemos como Máquina Universal de Turing". [153]

Casi en paralelo, un año después, en 1937, en su tesis doctoral, que desarrolló en el MIT, Shannon demostró que es posible expresar sentencias del álgebra de Boole mediante la combinación de relés y circuitos eléctricos. Ésta significó una gran contribución a la teoría de diseño de circuitos digitales.

Durante la Segunda Guerra Mundial Turing y Shannon dedicaron gran parte de sus investigaciones a la criptografía y al criptoanálisis. Como lo hemos mencionado, Turing desempeñó un papel importante en Bletchley Park donde, con otros matemáticos pudo descifrar los mensajes transmitidos por la máquina Enigma, usada por la marina alemana.[154] Shannon trabajó en los Laboratorios Bell de Nueva York donde, a partir del artículo *A Mathematical Theory of Communication* (1948), sentó las bases de la teoría de la información, y con el artículo *Communication Theory of Secrecy Systems* (1949), las bases de la criptología moderna.

De acuerdo con la mayoría de sus biógrafos, se podría inferir que al principio Turing y Shannon se sintieron poco interesados en el desarrollo de las computadoras y experimentaron otras vías de investigación coincidiendo, otra vez, en las máquinas que juegan al ajedrez, en la criptografía y en la comunicación

[153] David Hilbert denominó Entscheidungsproblem (problema de la decisión), al problema de hallar un método de cálculo que permita decidir mecánicamente para toda fórmula lógica si es o no válida. Una respuesta afirmativa a este problema podría implicar que todo problema matemático fuese mecánicamente resoluble.

[154] Aunque hay varios textos que explican la participación de los matemáticos, ingenieros, lingüistas, traductores y científicos de diversas áreas, uno de los más detallados y completos es *The Secrets of Station X. How Bletchley Park Helped Win the War,* de Michael Smith (2011).

secreta. En esa época Shannon publicó el artículo *Programming a Computer for Playing Chess (1949)*, donde d escribió c ómo u na computadora puede j ugar razonablemente aj edrez, poni endo el i nterés en l a r esolución automática d e problemas por encima de la importancia de que las máquinas pudieran "pensar".

Por otro lado, Turing, en s u artículo *Digital Computers Applied to Games (1951)*, se c uestionó s i l os j uegos c onstituían un m odelo i deal par a e l es tudio d e l a "inteligencia" de l as c omputadoras c onvirtiéndose as í en pr ecursor de l a inteligencia artificial.[155] Uno de sus paradigmas fue el denominado *Test de Turing* concebido para saber si un usuario de una computadora es un ser humano o una máquina.[156]

Además de algunos intereses comunes, entre sus coincidencias, hay que resaltar que l as l íneas d e i nvestigación s eguidas p or *Turing* y por *Shannon* han s ido trascendentes t anto p ara l as matemáticas c omo p ara l a c omputación y , au nque hasta ahora ha n s ido i gnoradas, t ambién par a l as TIC y l as c iencias d e l a comunicación. Habría que precisar, sin embargo, que a Turing le interesaba más lo r eferente a l a c omputabilidad y a Shannon, l o r elacionado a su t eoría de l a información.

En 1950, durante un congreso en Londres sobre cibernética, y en particular en la charla s obre 'Información, m áquinas y c erebro ", Turing defendió l a i dea de que "una m áquina deb e p oder al terar s us pr opias i nstrucciones", di stinguiendo es e concepto del de bifurcación condicional, que permite que el programa haga unas

[155] Tanto Turing como Shannon eligieron el ajedrez como campo de experimentación porque el número de partidas distintas posibles (un uno seguido de 123 ceros) es impráctico pero es finito para una computadora. Y ya intuyeron que para lograr su objetivo -ganar al campeón del mundo- no bastaría con el camino A (fuerza bruta tonta), sino que éste debería confluir con el B (más lento pero mucho más inteligente). Deep Blue ganó medio siglo después a Gari Kaspárov (número uno de 1985 a 2005) porque IBM logró que el silicio tuviera un algoritmo Alpha-Beta, cuya forma de pensar recordaba vagamente a la de un gran maestro: éste descarta en muy pocos segundos el 90% de las jugadas legales posibles, y se concentra sólo en el cálculo o evaluación de tres o cuatro.

[156] Los Test CAPTCHA (Completely Automated Public Turing Test *to Tell Computers and Humans Apart)*, con los que debemos escribir letras o signos confusos, son un test de *Turing* inverso, con los que un ordenador intenta distinguir entre una persona y una máquina para evitar accesos de autómatas.

cosas cuando se cumplen ciertas condiciones y otras en caso contrario [157], al mismo tiempo que recriminó que la teoría de la información de Shannon no tenía en cuenta el coste computacional.

Estas líneas de investigación se desarrollaron de forma independiente y complementaria: la de Turing asumiendo que los procesos de **almacenamiento** y **comunicación de datos** eran perfectos para conseguir la computabilidad y la de *Shannon* utilizando la **computación** (en los procesos de **codificación** y **decodificación**) para lograr el almacenamiento y comunicación de datos de la forma más fiable posible.

Además de su trabajo académico, Shannon fue asesor y consultor en el National Defense Research Committee de Estados Unidos y abarcó campos tan diversos como el uso del álgebra en circuitos, la teoría de la comunicación, las matemáticas y la criptografía así como el uso de computadoras para operaciones numéricas, juegos de ajedrez y máquinas (ratones electrónicos) para recorrer (resolver) laberintos.

En una entrevista, realizada en Winchester, M.A., por Robert Price el 28 de julio de 1982,[158] se explica la trayectoria de Shannon en la década de los años cuarenta del siglo pasado y su relación con Norbert Wiener y otros reconocidos matemáticos. Ahí narra su desarrollo como miembro del National Research Council y el Institute for Advanced Study durante la Segunda Guerra Mundial y su trabajo de investigación en los Laboratorios Bell, las influencias de Wiener en su trabajo y viceversa. Analiza sus reportes criptográficos de 1945 y la publicación en 1949 de su *Communication Theory of Secrecy Systems* así como su restricción debido a la Guerra. Explica su acceso al trabajo de John Tukey, William R. Bennett, John Riordan y el propio Alan Turing, así como su escasa relación con

[157] La bifurcación condicional es una de las estructuras de programación más importantes. Véase Glosario.
[158] Véase la entrevista de Robert Price a Shannon, (1982).

este último antes y después de la guerra, tanto en los Laboratorios Bell y en Princeton en Estados Unidos como en Inglaterra.

VI.2 Computadoras con programa almacenado ¿Turing y Shannon o alguien más?

Con el doctor Ricardo Peña, catedrático de la Universidad Complutense de Madrid,[159] comenzaremos diciendo que **"**Multitud de libros de informática afirman que el primer computador electrónico de la historia fue el ENIAC, desarrollado en la Moore School de la Universidad de Pensilvania, coincidiendo con el final de la II Guerra Mundial, y que el primer computador con programa almacenado fue el EDVAC desarrollado poco después. También que su diseño se debió al genio del matemático estadounidense de origen húngaro John von Neumann. Nuestros computadores actuales repiten las líneas esenciales de ese diseño y por eso hablamos frecuentemente de una arquitectura "tipo von Neumann" para referirnos a un computador convencional que ejecuta sus instrucciones de forma secuencial y que almacena su programa en la misma memoria que los datos".[160]

Es importante que se reconozca a Turing y sus contribuciones a la concepción y nacimiento práctico de las computadoras electrónicas, desconocidas durante años debido al secreto que impuso el Servicio de Inteligencia Británico a sus aportaciones durante la guerra y la posguerra. " Su artículo de 1936, *On Computable Numbers, with an Application to the Entscheidungsproblem*, fue la verdadera semilla de los computadores con programa almacenado. Aunque su propósito original era formalizar la idea de " procedimiento efectivo" que los matemáticos habían usado de manera informal, y su objetivo último era demostrar que no existía tal procedimiento para resolver el llamado "problema de decisión" (comprobar la veracidad o falsedad de cualquier fórmula lógica), el trabajo tuvo como resultado colateral de mostrar que existía una sola máquina, llamada

[159] Peña, Ricardo (2012).

[160] Véase también la estupenda recopilación de textos británicos sobre el tema, editado por Simon Lavington, *Alan Turing and his Contemporaries. Building the world"s first computers*, The Chartered Institute for IT, BISL, Chippenham, UK, 2016.

posteriormente *Maquina Universal de Turing,* capaz de calcular cualquier función computable. Una sola máquina podía en definitiva ejecutar cualquier algoritmo". (Lavington, 2016)[161].

Ese artículo, además de suponer una revolución en las matemáticas de la época, era perfectamente conocido, y apreciado en toda su profundidad, tanto por von Neumann como por Max Newman, el preceptor de Turing en Cambridge. Como hemos mencionado, durante la guerra, Max Newman dirigió la construcción de *Colossus*, una máquina electrónica que fue decisiva para descifrar los mensajes de la máquina alemana *Tunny*, con la cual se codificaban los mensajes del alto mando alemán. Gracias a ella, el día D (6 de junio de 1944) los aliados supieron que los alemanes no esperaban el gran desembarco en la costa de Normandía y ganaron unos días definitivos antes del contraataque alemán.

Si bien Turing contribuyó a la concepción teórica de *Colossus* con algunos algoritmos, otros matemáticos también participaron y el algoritmo principal se debió al criptógrafo Bill Tutte. Por otra parte, en el diseño electrónico y la realización práctica colaboraron otras mentes: el ingeniero Tommy Flowers fue quien utilizó por primera vez cientos de válvulas en una sola máquina. (Lavington, 2016).

A partir del éxito de *Colossus*, tanto Turing como Newman fueron conscientes de que la electrónica digital era el camino apropiado para la construcción física de una máquina universal programable. Hay que señalar que *Colossus* funcionó por primera vez a finales de 1943, mientras que ENIAC, la que se dice fue la primera computadora programable y con posibilidad de almacenar información, fue

[161] El propio Lavington explica que "Más aún, la descripción del algoritmo se podía almacenar de forma codificada en la misma cinta en la que se almacenaban los datos de entrada y los resultados intermedios y finales del cómputo. La cinta de una Máquina de Turing constituye, así, su memoria. La descripción a su vez constaba de un conjunto de instrucciones elementales, cada una de las cuales decidía, por un lado la acción a ejecutar, y por otro cuál debía ser la siguiente instrucción a ser ejecutada. Las acciones eran tan simples como leer o escribir un símbolo, y/o desplazar la cabeza lectora una posición en la cinta. Aquí aparecen ya todos los conceptos utilizados en un computador moderno con programa almacenado.

terminada hasta 1945. Ambas eran computadoras electrónicas de propósito específico, la primera para el desciframiento de mensajes y la segunda para el cálculo de trayectorias balísticas.[162] Aunque cambiar la programación exigía reconectar cables y modificar interruptores de forma manual, ambas eran en cierta medida programables.

Varios autores coinciden en que la razón por la que ENIAC es reconocida como la primera computadora electrónica de la historia es que tanto la existencia como la información sobre *Colossus* se fue desclasificando parcialmente y se hizo con mayor amplitud hasta los años setenta del siglo pasado, y en su totalidad hasta 2004. (Smith, 2011).

Al terminar la guerra, tanto Turing como Newman iniciaron la construcción física de una computadora. El primero en el National Physical Laboratory (NPL) en Londres, y el segundo en la Universidad de Manchester, también en Inglaterra. Paralelamente, en Estados Unidos el equipo original de ENIAC –(particularmente los ingenieros John Mauchly y John Eckert) al que se había incorporado von Neumann– inició el diseño de la EDVAC y enriqueció lo referente a su programación manual y a un programa almacenado en memoria[163]. Por problemas internos, el equipo se disolvió y el informe se distribuyó con la única firma de von Neumann. Independientemente de esto que condujo a un largo juicio en los tribunales sobre la autoría del concepto de computadora electrónica, aunque von Neumann nunca lo citó en el informe, sí conocía el artículo de Turing.

Por el contrario, el informe de Turing, *Proposed Electronic Calculator* (1945) y mucho más detallado que el de la EDVAC, donde exponía el diseño de su computadora ACE, sí citaba el informe firmado por von Neumann, diciendo que ambos "han de leerse conjuntamente". No pudiera firmarse que el diseño de EDVAC fuera la inspiración para el de Turing puesto que ambos diseños eran

[162] Importantes detalles sobre los avances y descubrimientos británicos se encuentran en los artículos "The ideas men" y "Oces and Deuces" de Simon Lavington en el libro ya citado el cual él editó.
[163] El informe *First Draft on a Report on the EDVAC,* publicado en junio de 1945, da cuenta de ese diseño.

distintos y mientras la ACE resolvía por ***software*** muchas operaciones, la EDVAC las delegaba al ***hardware***. (Lavington, 2016 y Smith, 2011).

Aunque estos momentos en la historia de la computación son confusos, se ha reconocido que Turing tenía pues su propia idea acerca de lo que debía ser una máquina universal programable. Por otra parte, está documentado que la idea de construir una computadora real con programa almacenado provocó frecuentes discusiones entre Turing y Newman en sus pocos momentos de interacción durante la guerra. Lo único que podemos constatar es que el informe sobre la EDVAC puso por primera vez por escrito la idea de almacenar el programa en memoria en una máquina real y no simplemente conceptual. (Lavington, 2016 y Smith, 2011).

En Inglaterra, Newman fue realmente el primero en completar la construcción de una computadora electrónica con programa almacenado. Se trató de la *Manchester Baby*, terminada en 1948, tres años antes que EDVAC, y que usaba como memoria un tubo de rayos catódicos. Tampoco Newman figura para la historia como el autor de esta máquina, que ha sido atribuida a Freddy Williams y a Tom Kilburn, ingenieros electrónicos que dirigieron su construcción. Como se documenta en *Colossus: The secrets of Bletchley Park's Codebreaking Computers* (Copeland, 2006) ambos fueron contratados por Newman e instruidos por éste y por Turing sobre el diseño de una computadora con programa almacenado. De hecho, Williams había sido inicialmente contratado por el NPL e instruido por Turing para colaborar en la construcción de la ACE, aunque el contrato se canceló al poco tiempo.[164]

Es necesario pues reescribir la historia y atribuir a cada uno sus propios avances y éxitos. La primera computadora electrónica de propósito específico fue *Colossus*

[164] La contribución de Williams y Kilburn fue sobre todo de ingeniería y muy en particular aportaron la realización por primera vez de una memoria sobre un tubo de rayos catódicos. En cambio, la EDSAC, completada en Cambridge por Maurice Wilkes un año después, y citada a veces como la primera computadora de programa almacenado, siguió las líneas de diseño del informe de la EDVAC y utilizó como ésta una memoria de líneas de retardo de mercurio.

en 1943 y no ENIAC, aunque es preciso acotar que los ingenieros de ENIAC desconocían la existencia de *Colossus* y se podría hablar por tanto de una reinvención del concepto.[165] Pero la idea teórica de una máquina universal programable con programa almacenado en memoria sí debe ser atribuida indudablemente a Turing. Podemos concluir que al acabar la guerra, la realización práctica de una computadora electrónica con programa almacenado fue un objetivo común de varios equipos de investigación. Tanto von Neumann, como Max Newman, Turing y Wilkes tenían ese propósito.

El informe sobre la EDVAC en 1945 aceleró sin duda los acontecimientos en el Reino Unido, que no quería quedarse atrás en esa carrera. En cuanto a los primeros en conseguirlo fue, sin duda, el equipo de Newman en Manchester en 1948, aunque se trató de una computadora con una memoria de tan solo 2.048 bits. La primera computadora con cierta capacidad de cómputo fue la EDSAC de Wilkes, en 1949.[166], que tampoco fue la primera máquina con programa almacenado en Estados Unidos, ya que Mauchly y Eckert completaron su máquina BINAC en 1949. Un prototipo de la ACE, aunque ya no con la participación de Turing, quien abandonó el proyecto en 1947, se completó en 1950 en el NPL. Turing tuvo también alguna influencia en el diseño de la máquina sucesora de la *Manchester Baby*, la Ferranti Mark I, completada en la Universidad de Manchester en 1951 (Peña, Ricardo).

VI.3 Archivos y cuadernos de Turing

El sitio del archivo de Turing en la Universidad de Cambridge, Inglaterra, que tuvimos la oportunidad de visitar en una práctica de campo en mayo-junio de 2018, contiene cerca de 30 00 imágenes de cartas, fotografías, artículos de periódicos y documentos originales de o sobre Alan Turing.[167] Los papeles de

[165] No obstante, también está documentado que el uso de válvulas para realizar cómputos ya estaba presente en la máquina inconclusa ABC de John Atanasoff, de la cual Mauchly tuvo conocimiento en una visita realizada a la Universidad de Iowa hacia 1941, antes de involucrarse en la ENIAC.

[166] La EDVAC, concebida por von Neumann, Mauchly y Eckert funcionó hasta 1951.

[167] Todas las imágenes están sujetas a leyes de derechos de autor; el catálogo completo está en línea e incluye detalles de su procedencia. Este catálogo fue conformado tanto por el Kings College como por el

Turing contienen documentos publicados e inéditos, públicos y personales escritos por el propio Turing y por sus colegas, amigos y otros autores. Se encuentran también cartas y su tesis para su beca. Muchos de los documentos de las secciones B, C y D se refieren al trabajo de Turing de 1940 hasta su muerte en 1954. En su correspondencia hay algunas referencias a su trabajo en la década de los treinta pero no hay borradores de dicho trabajo. En la sección D se encuentran algunas cartas de Turing escritas en Bletchley Park durante la guerra Mundial. En la Sección C/24-27 hay documentos sobre morfogénesis, área de trabajo que Turing dejó incompleta tras su muerte. La Sección D contiene cartas fotocopiadas y cálculos compartidos entre Turing y I. J. Good (D/6-10) y cartas originales dirigidas a P. Hall. La Sección E contiene grabaciones de video y copias de las conferencias dictadas en el Turing Celebration Day en octubre de 1997.

La madre de Turing, quien le sobrevivió por varios años, escribió una biografía de 157 páginas de su hijo, que fue publicada en 1959. Se vendieron sólo 300 ejemplares. Con un prólogo de seis páginas de Lyn Irvine incluye reminiscencias y es frecuentemente citado. (Sara Turing y Lyn Newman, 1967). Fue republicado por Cambridge University Press en 2012 en honor al centenario de su nacimiento, y se incluye un nuevo prólogo de Martin Davis, así como memorias nunca antes publicadas del hermano mayor John F. Turing. Todos los derechos de reproducción pertenecen al NCUACS y al Kings College de la Universidad de Cambridge. Los archivos se encuentran en seis cajas y la fecha de adquisición y la fuente son: 1960 (K/1-7).[168]

National Cataloguing Unit for the Archives of Contemporary Scientists (NCUACS) y el Turing Trust e incluso por donaciones de su madre Sara Turing.

[168] En junio de 1960, la Sra. Sara Turing, madre y biógrafa de Alan, llevó algunos documentos de su hijo al Kings College, listado preliminar al de 1977. Algunos objetos (como un corta papales y algunas cartas). Su catalogación es A/1-13; B/1, 3-7; D/1-5). En 1975, se estableció el A.M. Turing Trust como una entidad para el avance y desarrollo educativo en campos como la computación, la inteligencia artificial y lógica matemática. El material de las secciones 1960-77: A7/1-13; B/1, 3-7; D/1-5 fue reunido por este Trust.
Los manuscritos archivados en las secciones C/1-22 son inéditos y fueron reunidos después de la muerte de Turing por el Dr. Robin Gandy, nombrado su heredero en su testamento (en A/5). En las secciones 1984-96 hay varios documentos de menor importancia provenientes de distintas fuentes y en distintos estados: originales, borradores, publicados y cartas y notas personales.

En 1977, el heredero de Turing, Gandy donó los documentos de Turing a los archivos de King's College en la Universidad de Cambridge pero conservó, hasta su muerte en 1995, un cuaderno casi desconocido del matemático británico que fue subastado hace pocos años en Nueva York.

El cuaderno de apuntes de 56 páginas, escrito a mano por Turing, que se vendió en más de un millón de dólares a un comprador anónimo[169], fue escrito en el tiempo en que el matemático británico estaba trabajando para descifrar el aparentemente indescifrable código Enigma. El cuaderno contiene complejas anotaciones matemáticas y de ciencias computacionales de Turing, y se cree que es el único manuscrito extenso conocido de Turing que existe, según la casa Bonhams, que lo subastó.[170]

Al descifrar los códigos secretos de la máquina Enigma, con la que la marina de Alemania enviaba a sus submarinos mensajes para interceptar los convoyes de abastecimiento que Estados Unidos enviaba a Inglaterra, Turing utilizó en su trabajo conceptos de la hoy llamada inteligencia artificial y diseñó un a computadora electromecánica para simular las posibles combinaciones de letras de Enigma. Tras la guerra, en una época sin chips ni transistores, Turing diseñó las bases de una máquina programable que podía resolver operaciones.

Turing también ideó un lenguaje de programación con el que se podía simular todos los pasos que puede ejecutar una máquina siendo el primero en dar una noción precisa de lo que es un ***algoritmo***. Fue un visionario, que estableció

[169] El precio de venta fue de 1.025.000 dólares, unos 620 millones de pesos. La casa Bonhams que realizó la subasta dijo que el comprador quiso permanecer anónimo. El manuscrito de Turing data de 1942, cuando el matemático había sido reclutado por los servicios de seguridad para trabajar en Bletchey Park, como hemos asentado, el centro donde se realizaban los trabajos para descifrar los códigos utilizados por los nazis durante la Segunda Guerra Mundial. Los expertos en Turing esperan que el manuscrito ahora subastado no permanezca escondido otra vez durante décadas, sino que pueda ser estudiado en busca de pistas para comprender mejor la mente y la personalidad del matemático.

[170] El psiquiatra de Gandy le sugirió que escribiera sus sueños y él lo hizo en algunas de las páginas en blanco del cuaderno de Turing, su mentor, donde se lee: "Parece un camuflaje adecuado escribir entre estas notas de Alan, posiblemente es algo un tanto siniestro; es una figura paterna algunos de cuyos pensamientos he heredado completamente".

además el primer modelo teórico de lo que conocemos actualmente como aprendizaje de máquinas. Desarrolló el llamado test de Turing, que permite probar la existencia de inteligencia en una máquina. "Una computadora puede ser llamada inteligente si logra engañar a una persona haciéndola creer que es un humano", escribió (Valek, 2010).

Como vimos en capítulos anteriores, Turing es el precursor de la informática moderna por lo que se le considera uno de los padres de la ciencia de la computación y proporcionó una influyente formalización de los conceptos de algoritmo y computación: la máquina de Turing.[171] Como hemos mencionado, durante la Segunda Guerra Mundial, como director de la sección Naval Enigma del Bletchley Park trabajó en romper los códigos nazis, particularmente los de la máquina Enigma. Tras la guerra diseñó una de las primeras computadoras electrónicas programables digitales en el Laboratorio Nacional de Física del Reino Unido y poco tiempo después contribuyó a la construcción de las primeras máquinas en la Universidad de Manchester.

Parte esencial del cálculo es, evidentemente, el uso de reglas. En un sentido más preciso, sin embargo, convenimos en decir que algo es efectivamente calculable o computable si existe un algoritmo 2 o procedimiento de decisión o procedimiento efectivo que lo resuelva, entendiendo por tal un método o procedimiento que se efectúa conforme a reglas y que permite resolver un conjunto de problemas de una manera mecánica y en un número finito de pasos.

La caracterización matemática del concepto de lo computable tuvo lugar en esos años a lo largo de líneas independientes de investigación que han conducido, sin embargo, a resultados convergentes. En una de ellas se sitúa la teoría elaborada por Turing, cuya teoría ya mencionada " Sobre números computables, con una aplicación al problema de la decisión" es ya un texto clásico en la lógica

[171] Recordemos que formuló su propia versión de la Tesis de Church-Turing, la cual postula que cualquier modelo computacional existente tiene las mismas capacidades algorítmicas, o un subconjunto, de las que tiene una máquina de Turing.

contemporánea. La parte nodal de esta teoría es la descripción de un tipo de máquinas abstractas de estructura conceptualmente muy simple, pero capaces de realizar complicadas funciones de computables.[172]

"Para Turing el cálculo se efectúa normalmente escribiendo símbolos en un papel. Podemos suponer que este papel se divide en cuadrados, como el cuaderno de aritmética de un niño. En aritmética elemental se aprovecha a veces el carácter bidimensional del papel. Pero se puede prescindir de ese uso, que no es esencial para la computación. El comportamiento de la persona que calcula está en todo momento determinado por los símbolos que está observando y por su "estado mental" en ese momento. Podemos suponer que el número de símbolos o cuadrados que puede observar en un momento tiene un límite. **"**Supondremos también que el número de estados mentales a tener en cuenta es finito [ ] Tampoco esta restricción afecta seriamente a la computación, porque el uso de estados mentales más complicados se puede suplir escribiendo más símbolos en la cinta'… Una es la analogía que guarda la conducta de la máquina con el comportamiento del calculador humano, que, en el proceso de cálculo, depende en cada momento de los símbolos que observa y de su estado mental (su conocimiento y memoria de las reglas de cálculo y de la marcha anterior del proceso) en ese preciso momento. Y eso es, advierte Turing, lo que sucede con la máquina: el posible comportamiento de la máquina en cualquier momento está determinado por su estado y el símbolo escrutado. (Garrido, Manuel, *2008:* 375-392).

VI. 4 Sistemas secretos de Shannon

La *Teoría de la comunicación de los sistemas secretos* es uno de los tratamientos fundacionales sobre la criptografía moderna. Fue escrita en 1949 por Claude E. Shannon y se refiere a la criptografía desde el punto de vista de la teoría de la

[172] Los lógicos que investigaban hacia los años treinta en el marco del problema hilbertiano de la decisión abordaron la tarea más ambiciosa de caracterizar o codificar exactamente, en los términos de una teoría matemática precisa, el concepto de lo efectivamente computable o calculable. El resultado ha sido una de las principales aportaciones de la lógica matemática de nuestro siglo, la creación de un área de conocimiento enteramente nueva, la teoría general de la computabilidad.

información. Es también una prueba de que todos los cifrados indescifrables en teoría tienen que tener los mismos requisitos que una libreta de un solo uso.[173] Según Shannon, para hacer un algoritmo de cifrado más resistente es necesario que cumpla con la difusión y confusión. De esta forma se reducía considerablemente la posibilidad de detectar el algoritmo por análisis de frecuencias.[174]

De esa manera, la **difusión** implica que si se cambia un bit en el texto sin cifrar, deberían cambiarse la mayor cantidad posible de bits en el texto cifrado. Para conseguir este efecto se realizan las permutaciones. La **confusión,** por su parte, significa que la relación entre el texto cifrado y la clave es lo más compleja posible. Las sustituciones cumplen con ese objetivo.[175]

En criptografía, la libreta de un solo uso (del inglés *one-time pad*), es un tipo de algoritmos de cifrado por el que el texto en claro se combina con una clave aleatoria o *"libreta"* igual de larga que el texto en claro y que sólo se utiliza una vez. Se inventó en 1917. Si la clave es verdaderamente aleatoria, nunca se reutiliza y, por supuesto, se mantiene en secreto, se puede demostrar que el método de la libreta de un solo uso es indescifrable.[176]

Algunos autores emplean el término "cifrado de Vernam" como sinónimo de "libreta de un solo uso", mientras que otros lo utilizan para cualquier cifrado de flujo aditivo, incluyendo los basados en un generador de números

[173] Shannon publicó una versión más temprana de esta investigación en el informe clasificado *Una Teoría Matemática de Criptografía*, Memorándum MM 45-110-02, Sept. 1, 1945, Laboratorios Bell.[1]. Este informe clasificado también precede a la publicación de su "Una teoría matemática de la comunicación" de 1948.

[174] **Confusión y difusión** son dos conceptos relacionados con la teoría de la información y de la comunicación. Shannon, uno de los padres de esta teoría, participó con ciertos postulados acerca de los sistemas de cifrado.

[175] Horst Feistel en 1971 trabajó en el proyecto Lucifer de IBM, proyecto en el que nace la estructura de feistel, que incorpora el pensamiento de Shannon acerca de la difusión y confusión, de manera que se aplicaron permutaciones y sustituciones respectivamente para producir estos efectos

[176] La parte del nombre relativa a la «libreta» procede de las implementaciones iniciales en las que la clave se distribuía en forma de libreta de papel, de manera que la página podía romperse y destruirse tras su uso. Para facilitar la ocultación, a veces la libreta era físicamente muy pequeña.

pseudoaleatorios criptográficamente seguro. [177] Al principio se reconocía que la libreta de un solo uso de Vernam-Mauborgne era muy difícil de romper, pero su estatus especial fue descubierto por Shannon unos 25 años después. Usando elementos de la teoría de la información, demostró que la libreta de un solo uso tenía una propiedad que él llamó *secreto perfecto*: es decir, el texto cifrado no proporciona información acerca del texto en claro. Y de hecho todos los textos en claro son igualmente probables. Esto es una poderosa noción de dificultad criptoanalítica.

A pesar de la demostración de Shannon, la libreta de un solo uso tiene en la práctica desventajas: requiere libretas de un solo uso perfectamente aleatorias; la generación e intercambio de las libretas de un solo uso tiene que ser segura, y la libreta tiene que ser al menos tan larga como el mensaje; hace falta un tratamiento cuidadoso para asegurarse de que siempre permanecerán en secreto para cualquier adversario, y es necesario deshacerse de ellas correctamente para evitar cualquier reutilización. Estas dificultades de implementación han evitado que la libreta de un solo uso haya sido adoptada como una herramienta generalizada de seguridad informática.

En particular, el uso único es absolutamente necesario. Si una libreta de un solo uso se utiliza tan sólo dos veces, unas sencillas operaciones matemáticas pueden reducirla a un cifrado de clave corrida. Si ambos textos en claro están en lenguaje natural (por ejemplo, en inglés o en ruso), aunque ambos sean secretos, hay muchas posibilidades de que sean recuperados con criptoanálisis, posiblemente con algunas ambigüedades.[178]

[177] El sistema de Vernam, creado por Gilbert Vernam, era un cifrado que combinaba un mensaje con una clave que se leía de un bucle de cinta de papel. En su forma original, el sistema de Vernam no era irrompible porque la clave se podía reutilizar. El uso único se dio cuando Joseph Mauborgne reconoció que si la cinta de la clave era completamente aleatoria, se incrementaría la dificultad criptoanalítica.

[178] La libreta de un solo uso no proporciona ningún mecanismo para asegurar la integridad del mensaje, y en teoría un atacante en el medio que conozca el mensaje exacto que se está enviando podría sustituir fácilmente parte o todo el mensaje con un texto de su elección que sea de la misma longitud. Se pueden usar las técnicas estándar para evitar esto, como un código de autentificación de mensaje, pero carecen de la prueba de seguridad de la que gozan las libretas de un solo uso.

Las libretas de un solo uso son seguras desde el punto de vista de la teoría de la información, en el sentido de que el mensaje cifrado no le proporciona a un criptoanalista información sobre el mensaje original. Esta es una poderosa noción de seguridad, desarrollada y demostrada matemáticamente por primera vez durante la Segunda Guerra Mundial por Shannon.[179]

Para explicar la libreta de uso único es necesario distinguir entre dos nociones de seguridad. La primera es la seguridad teórica del sistema de libreta de uso único demostrada por Shannon. La segunda es la seguridad ofrecida por los cifrados más punteros (por ejemplo, el AES) diseñados con los principios aprendidos durante la larga historia de la rotura de códigos y sujetos al testeo intensivo en un proceso de estandarización, bien en público o por un servicio de seguridad de primera clase (seguridad empírica). La primera está demostrada matemáticamente y está sujeta a la disponibilidad práctica de los números aleatorios. La segunda no está demostrada pero recibe la confianza de la mayoría de los gobiernos para proteger sus secretos más vitales.

Si la clave la genera un programa determinista, entonces no es aleatoria ni se puede afirmar que el sistema de cifrado ofrezca la seguridad teórica de la libreta de un solo uso. Se llama cifrado de flujo.

Los cifrados *Fish* usados por el ejército alemán en la Segunda Guerra Mundial resultaron ser cifrados en flujo inseguros, no útiles libretas de un solo uso automatizadas como pretendían sus diseñadores. En Bletchley Park se rompía uno de ellos regularmente, la máquina de cifrado de Lorenz. (Smith, 2011).

Shannon desarrolló fórmulas que permiten al criptoanalista saber cuándo una solución en un sistema de cifrado particular es válida. *Discute el* secreto perfecto

[179] Sus resultados fueron publicados en el *Bell Labs Technical Journal* en 1949. Las libretas de un solo uso, utilizadas adecuadamente, son seguras en este sentido incluso contra adversarios con poder computacional infinito.

(absolutamente cifrado irrompible) y el secreto ideal (cifrados prácticamente irrompibles) y las características de trabajo necesarias para resolver diferentes tipos de cifrado. Además de ser el fundador del campo de la teoría de la información, mostró la base teórica y práctica para los circuitos digitales (1938), la base matemática para internet (1948) y un trabajo fundamental en criptografía. Shannon incluso escribió un documento sobre ajedrez de computadora y fue nombrado consultor en asuntos criptográficos para el Gobierno de los Estados Unidos. El trabajo presentado en este documento apareció originalmente en un informe confidencial '' Una Teoría Matemática de la Criptografía fechada el 1 de septiembre de 1945 pero clasificada en ese momento debido a la Segunda Guerra Mundial.[180]

En 1938 Shannon probó que los circuitos podían usarse para simplificar los arreglos electromecánicos para rutas telefónicas. Luego amplió este concepto probando que esos circuitos podrían resolver todos los problemas que el álgebra booleana podía resolver. Presentó diagramas de varios circuitos, usando la propiedad de los interruptores eléctricos para implementar lógica como concepto fundamental que subyace a todas las computadoras electrónicas digitales. El trabajo de Shannon resulta fundacional en el área del diseño digital.

En los Laboratorios Bell Shannon trabajó en los sistemas de control de fuego y criptografía bajo un contrato con la sección D-2 (sección de sistemas de control del National Defense Research Committee (NDRC). Se le acredita la invención de gráficas de flujo de señales en 1942. Descubrió la fórmula topológica mientras investigaba la operación funcional de una computadora analógica.

En 1943, durante dos meses, estuvo en contacto con Turing, quien había sido asignado a Washington para compartir con el servicio criptoanalítico de la marina estadounidense los métodos usados en el British Government Code and Cypher

[180] Véase Claude Shannon, 1949. "Communication Theory of Secrecy Systems". *Bell System Technical Journal* 28, 4: 656-715.

School en Bletchley Park para descifrar los códigos usados por el submarino Kriegsmarine en el norte del océano Atlántico y mostró a Shannon su documento de 1936, donde definía su Máquina Universal de Turing, esto impresionó a Shannon pues complementaba muchas de sus ideas.

Terminada la guerra, preparó un memorándum clasificado para los Laboratorios Bell titulado "A Mathematical Theory of Cryptography (Septiembre de 1945). Una versión desclasificada de este documento se publicó en 1949 como "Communication Theory of Secrecy Systems" en el *Bell System Technical Journal*, que incorporó muchos conceptos y fórmulas matemáticas que también aparecieron en su *A Mathematical Theory of Communication*.

Mientras estaba en los Laboratorios Bell, Shannon probó que la criptografía de una libreta de uso único (*cryptographic one-time pad*) es irrompible (indescifrable) También demostró que cualquier sistema indescifrable debe tener esencialmente las mismas características que uno de un solo uso: la clave debe permanecer oculta, ser tan larga como el propio texto y nunca reusarse completa o en partes y mantenerse secreta.

En capítulos anteriores definimos a la criptografía como la práctica y estudio de técnicas para asegurar la comunicación en presencia de terceros (llamados adversarios). Sus aplicaciones incluyen tarjetas bancarias y comerciales y uso gubernamental. Se ha usado también y sobre todo como espionaje por lo que se ha clasificado como herramienta, arma y se ha limitado e incluso prohibido su uso. Un cifrado es un par de algoritmos que crean un encriptado, la operación de un cifrado es controlada por un algoritmo y en cada instante por una clave secreta.

Dentro de su trabajo en la Guerra, Shannon contribuyó enormemente a desencriptar mensajes secretos a través de su teoría de la criptografía. Aunque el trabajo de Shannon en IA ha sido comúnmente ignorado, sabemos que intervino incluso en la definición del concepto. En 1956 dejó los Laboratorios Bell por el

MIT, primero como profesor invitado y luego como miembro permanente del Laboratorio de Investigación en Electrónica. Duró en ese puesto 20 años, desde 1959, después de disfrutar una beca en el Centro de Estudios Avanzados en Ciencias del Comportamiento en Palo Alto. Fue invitado a la URSS para dar una conferencia en un congreso de ingeniería, donde tuvo la oportunidad de jugar ajedrez con Mikhail Botvinik. Abordó posteriormente el caso de la transmisión a través de canales sin memoria (un canal ruidoso en el que el ruido actúa independientemente sobre cada símbolo transmitido), tema sobre el que publicó su último artículo en teoría de la información (en 1967, con Robert G. Galler y Edwin R. Berlekamp).

Específicamente con respecto a la inteligencia artificial. Shannon fue coautor del "Proposal for the Dartmounth Summer Research Project on Artificial Intelligence" (Propuesta para el proyecto de investigación Dartmounth Summer en inteligencia artificial) de 1955, que supuso el nacimiento del término "inteligencia artificial". Junto a Nathaniel Rochester, John McCarthy y Marvin L. Minsky obtuvo apoyo de la Fundación Rockefeller para "proceder sobre la base de la conjetura de que todo aspecto del aprendizaje o cualquier otra característica de la inteligencia puede en principio ser descrito con tanta precisión que una máquina pueda simularlo." Al explicar su propio objetivo Shannon mencionó dos asuntos.

El primero, presentado como una aplicación de la teoría de la información, se basaba en una analogía: de la misma manera que la teoría de la información estaba implicada en la transmisión fiable de información sobre un canal ruidoso, deseaba aquí abordar la estructura de las máquinas de computación en la que se supone que una computación fiable puede lograrse mediante algunos elementos no fiables; a este problema algunos matemáticos como John von Neuman prestaron gran atención. A partir de este paralelismo, nociones tales como redundancia y capacidad de canal se usarían para mejorar la arquitectura de las máquinas de computación.

El segundo asunto se relacionaba con la manera en la que un “modelo de cerebro” puede adaptarse a su entorno. Esto no tenía una relación directa con la teoría de la información, sino que estaba más bien relacionado con el trabajo que Shannon presentó durante el VIII Encuentro Macy, en marzo de 1951, donde el matemático e ingeniero estadounidense mostró un ratón electromecánico que sería “instruido” para encontrar su camino en un laberinto.

En la propuesta de Dartmouth, Shannon puso énfasis en clarificar el modelo y representarlo como una estructura matemática. Ya había observado que “al discutir inteligencia mecanizada, pensamos en máquinas realizando las actividades de pensamiento humano más avanzadas —aportando teorema, escribiendo música, o jugando ajedrez. Postuló una aproximación abajo-arriba en la dirección de estas actividades avanzadas, empezando con modelos simples, como había hecho en su artículo de 1950 titulado “Programming a Computer for Playing Chess” (Programando un ordenador para jugar al ajedrez). En este primer artículo publicado sobre ajedrez computacional, Shannon ofrecía los elementos clave para escribir un “programa,” tal como un a “función de evaluación” o un “procedimiento mini-max.”

En el siglo XXI Shannon hizo múltiples contribuciones al desarrollo de la computación pues también hay un gran número de nuevos campos que no podrían definirse sin referencia a su obra. En el campo tecnológico, teorías de código que se aplican a la comunicación son meros desarrollos de la teoría de la información. En matemáticas, partes enteras de la teoría de complejidad algorítmica se deben a los desarrollos de la teoría shannoniana. En biología, el uso multiforme de la expresión “información genética” explica el desarrollo de la biología molecular (Fox Keller, Kay y Jockey). Desde la década de 1990 en adelante, en física, el dominio de la “información cuántica” despegó en torno a la

definición de *qubits*, que extiende el *bit* inicialmente usado por Shannon para medir la información. (Segal, 2010).[181]

Después de entrelazar las vidas y aportaciones de Turing y de Shannon a las ciencias de la comunicación, a la comunicación secreta y a las TIC durante los primeros sesenta años del siglo XX en el mundo anglosajón tanto en Europa como en América, terminamos este capítulo con el propósito, insistimos, de incorporarlos a nuestros proyectos de investigación y programas académicos y de ubicar cabalmente la comunicación secreta y a la criptografía computacional a nuestros planes de estudio.

[181] Corresponde con la versión actual del artículo del autor editado en versión inglesa en febrero de 2009 y traducida por J.M. Díaz en enero de 2010.

CONCLUSIONES

El recorrido metodológico que realizamos en este trabajo de investigación con las herramientas que nos proporcionó la hermenéutica profunda nos permitió vislumbrar a detalle las vidas y obras de Turing y de Shannon y ubicarlos en sus contextos específicos, capítulos I y II.

También nos permitió comprobar la omisión de ambos así como de la comunicación secreta y de la criptografía computacional en los modelos teóricos de las ciencias de la comunicación (capítulo III) y el estudio de las TIC (capítulo IV).

Como un objetivo posterior a este trabajo de tesis, proponemos definir cómo empezar a incorporarlos a los programas de estudio y proyectos de investigación de las ciencias sociales y específicamente de la comunicación y cómo sumar en ellos a la comunicación secreta.

Primero recapitulemos. En este trabajo se especificaron las aportaciones de Turing y de Shannon a lo que se denominó *comunicación secreta*, criptografía computacional y TIC y se expuso su relevancia en las ciencias de la comunicación a partir del método hermenéutico. También se puso en relieve la omisión de la que han sido objeto ambos científicos y sus descubrimientos en los programas académicos y de investigación dentro del campo de estudio de la comunicación.

Partimos de que la *comunicación secreta* es un fenómeno comunicativo, resultado y objeto de la criptografía computacional, que implica una *acción comunicativa* en la que los actores (emisor-receptor) buscan entenderse, excluyendo a quienes no posean su llave (clave) de decodificación.

En este sentido, se trabajaron tres ejes temáticos fundamentales que proporcionaron el marco conceptual para abordar nuestra investigación como

fenómeno de comunicación: el contexto histórico y científico en el que se desenvolvieron Turing y Shannon; la vida y obra de ambos con énfasis en sus aportaciones a la criptografía moderna o computacional, la comunicación secreta y la información y las tecnologías de la información y comunicación (particularmente con respecto a la computación).

Pusimos en relieve que las aportaciones de ambos científicos han sido abordadas y reconocidas ampliamente desde campos conceptuales de las matemáticas, la ingeniería y específicamente desde las ciencias de la computación pero no desde las ciencias sociales y el estudio de las nuevas tecnologías de la información, las plataformas digitales en redes electrónicas, de la comunicación en general y particularmente de un campo poco estudiado de ella, la comunicación secreta. Fue pertinente pues ubicarlos en su justa dimensión desde las ciencias de la comunicación y se hizo a través de la divulgación de sus aportaciones a partir de las tres categorías básicas de este análisis: el tiempo, el espacio y el momento coyuntural de la Segunda Guerra Mundial.

Dado que esta investigación buscó revaluar desde la hermenéutica la importancia de las obras de Turing y de Shannon respecto de la evolución de uno de los campos problemáticos más innovadores de las ciencias de la comunicación contemporánea (las TIC), trazamos los nexos que las unen al problema de la codificación del lenguaje, a través de nuestros cuatro ejes conceptuales fundamentales: **la criptografía computacional, el concepto de información, la comunicación secreta** y **las TIC.**

Al desentrañar los orígenes y el conjunto de condiciones históricas, intelectuales y científicas que permitieron y al mismo tiempo impulsaron a Turing y a Shannon a establecer las bases y condiciones de desarrollo de las TIC que hoy forman parte central del objeto de estudio de las ciencias de la comunicación, logramos revalorar en su justa dimensión su importancia en nuestra área de estudio. Para ello, en los capítulos iniciales de esta investigación primero hicimos un recorrido

fenomenológico por la vida y contexto sociopolítico en el que se desenvolvieron; segundo, conformamos y analizamos el corpus teórico sobre y alrededor de las TIC y tercero, logramos una construcción teórica que nos permitió ubicar a Turing y a Shannon en las TIC, tanto en sus raíces y aspectos teóricos como en sus aplicaciones prácticas, hoy fundamentales para las ciencias de la comunicación. Finalmente, en los últimos apartados de este trabajo, dimos pie a la aportación principal de esta investigación: ubicamos a la comunicación secreta y a la criptografía como importantes campos problemáticos inherentes a las ciencias de la comunicación, que han sido omitidos en nuestros programas y áreas de estudio.

Así, esta investigación es una *reconstrucción crítico interpretativa de las condiciones históricas* (contexto) que permitieron al matemático británico y al ingeniero estadounidense plantear las bases para el desarrollo de la criptografía computacional, la comunicación secreta y las TIC en la primera mitad del siglo XX y su trascendencia en el marco general de la comunicación social. Se revaluó, en pocas palabras, la importancia de ambos científicos en las ciencias sociales y específicamente en las ciencias de la comunicación.

Esto se hizo porque estamos convencidos de que comprender las tecnologías que operan como soporte material del discurso y que permiten su pluralización y extensión social, supone entender (comprender) a quienes bajo circunstancias históricas, políticas y culturales específicas, concibieron, diseñaron y sentaron las bases para el surgimiento y desarrollo de esas tecnologías.

Por otra parte, constatamos que el periodo en el que Turing y Shannon trabajaron ocurrió en un momento histórico convulso y singular en el que ellos participaron activamente: el momento coyuntural de la Segunda Guerra Mundial, en el que literalmente se puso en juego la supervivencia de la cultura occidental y con ésta muchos de sus valores fundamentales (entre ellos, el del conocimiento científico, la libertad de expresión y el derecho a la información). Conforme más avanzábamos en el análisis, nos pareció cada vez más pertinente estudiarlos,

contextualizarlos, entenderlos, interpretarlos y reinterpretarlos y que mejor forma de hacerlo que a partir de la hermenéutica, reflexión metodológica que, de acuerdo con sus principales exponentes, permite comprender ampliamente en su contexto el fenómeno a interpretar. En nuestro caso, contextualizamos nuestros problemas de investigación a partir de la historia, las aportaciones y biografías de los involucrados lo que nos permitió conocer con mayor objetividad los hechos y fenómenos sociales estudiados.

En esta investigación, partimos del supuesto de que los procesos sociales contemporáneos de comunicación, que alternan la mediación dialógica con la mediación tecnológica, están profundamente ligados a las obras de Alan M. Turing y de Claude E. Shannon. Dicha hipótesis general fue comprobada en cada uno de los capítulos que conforman este trabajo pues fueron principalmente ellos quienes desarrollaron tanto los fundamentos teóricos de las ciencias de la computación como los principios operativos fundamentales de lo que hoy denominamos TIC.

A lo largo de este trabajo de investigación vimos cómo Alan M. Turing proporcionó los fundamentos matemáticos, los modelos y los algoritmos que apuntan el uso de mecanismos electrónicos para cifrar y descifrar códigos y mensajes y almacenar y transmitir información mediante principios análogos a la comunicación humana.

También comprobamos cómo Claude E. Shannon sentó lo que desde la corriente funcionalista se consideran las bases de la teoría convencional de la información, generando un modelo matemático que permitió formalizar aspectos mecánicos de la transmisión/recepción de señales en determinados entornos electromagnéticos.

Así, al construir el contexto general del tema y ubicar a los autores, conceptos, nociones y textos sobre los distintos subtemas, cumplimos con el objetivo general de esta investigación al analizar y contextualizar, desde la perspectiva de una historia de las tecnologías de la información y de la comunicación, las aportaciones fundamentales de dos de los científicos más influyentes del siglo XX,

para la creación, consolidación y desarrollo de una nueva cultura en la que el lenguaje, la tecnología y la sociedad convergen para dar forma al perfil de la llamada sociedad de la información y a las TIC.

En ese sentido, recordamos que la intención de esta investigación no fue profundizar en el desarrollo o en los usos sociales de las TIC, sino en sus orígenes y, particularmente, en el conjunto de condiciones históricas, intelectuales y científicas que permitieron y, al mismo tiempo, impulsaron a Turing y a Shannon a establecer las bases y condiciones de posibilidad de las tecnologías que, en su parte social, no técnica ni matemática, hoy forman parte central del objeto de estudio de las ciencias de la comunicación.

Como argumentamos a lo largo de este trabajo, comprobamos que, mediante sus investigaciones secretas y su afán por romper esquemas y traspasar límites, Turing fue pionero al desarrollar teorías, instrumentos y máquinas de decodificación del lenguaje que sentarían las bases computacionales de lo que hoy son las TIC, sin las cuales hoy no se podría entender el mundo actual. Por tanto, este científico, al que se ignora en los estudios de comunicación, debería ser uno de los pilares de nuestro bagaje teórico. Tampoco podrían haberse desarrollado dichas tecnologías sin los innovadores trabajos criptográficos planteados por Shannon y, mucho menos, sin la Teoría matemática de la información planteada por el mismo ingeniero estadounidense y que, aunque algunas teorías reconocen, ha sido fuertemente criticada y no se le es da la importancia merecida.

A lo largo de este trabajo incorporamos los conceptos y las categorías que nos parecieron pertinentes para hacer visible el nexo que existe entre las aportaciones de Turing y las de Shannon a la comunicación secreta, a la criptografía computacional y a las TIC. Cabe mencionar que el análisis hermenéutico del impacto de las aportaciones criptográficas de Turing y de Shannon a las TIC,

específicamente en cuanto al desarrollo de los códigos binarios y de la computadora, se realizó con base en las nociones de ***programa*** y ***algoritmo***.

Como se especificó en reiteradas ocasiones, nuestro punto de atterrizaje metodológico se centró en "La metodología de la interpretación" de John B. Thompson donde, con base en el trabajo de otros teóricos demuestra que la *hermenéutica profunda* permite un marco en el cual se pueden interrelacionar diferentes métodos de análisis y hacer visibles sus ventajas y límites proporcionando un marco metodológico general. Con Thompson retomamos a Dilthey, Heidegger, Gadamer y Ricoeur para mostrar el papel relevante de la hermenéutica en la investigación sociohistórica. Con la hermenéutica partimos de que muchos fenómenos son formas simbólicas que suscitan problemas de comprensión e interpretación y que en particular en las ciencias sociales el objeto de nuestras investigaciones es en sí mismo un campo preinterpretado (Thompson, 2012).

Tomamos en cuenta la emisión de mensajes basados en códigos, que modifican la semántica de un lenguaje ya dado o generan una nueva semántica mediante la recodificación y pueden ser considerados subyacentes o metalenguajes (generados, artificiales, no naturales). En los capítulos II y III, momentos en que fue necesario para los fines de esta investigación, con Eco (2001) y Miller retomamos al código como un sistema de símbolos que por convención previa está destinado a representar, a transmitir la información desde la fuente al punto de destino.

Específicamente, con respecto a Alan Mathison Turing comprobamos que, además de ser un destacado matemático y lógico, sin sus trabajos de investigación, desarrollados en la primera mitad del siglo XX, las actuales tecnologías o plataformas sobre las que operan Internet, las redes sociales y en general todo lo relativo a sistemas de cómputo electrónico, no hubieran tenido un desarrollo tan acelerado y un despliegue tan amplio.

Por su parte, constatamos que a Claude Elwood Shannon se le reconoce ampliamente desde la ingeniería y la computación (incluso con algunos premios e instituciones que llevan su nombre) pero tampoco han sido valoradas a cabalidad sus aportaciones a las ciencias de la comunicación pues su conocida Teoría de la Información, a la que dedicamos varios apartados, creó falsas expectativas y se le exigió en su momento abarcar campos sociológicos que escapaban de su interés y áreas de estudio.

A partir de la investigación bibliográfica y documental plasmada en las páginas precedentes analizamos, interpretamos y reinterpretamos las vidas y obras de ambos teóricos, específicamente con respecto a sus aportes a la comunicación secreta, a la criptografía computacional y a las TIC. Con respecto al matemático británico nos adentramos en su concepción de la llamada *prueba de Turing* y en el diseño y desarrollo de la *Bomba*, máquina eletromecánica con la que le fue posible determinar la posición inicial de los rotores y funcionamiento de la máquina alemana Enigma.

Además de varios textos académicos, retomamos a los principales biógrafos de Turing, especialmente a Andrew Hodges (2012), quien lo rescató del olvido y a Rafael Lahoz-Beltrá (2005), que plantea la participación del matemático inglés en el desarrollo de Colossus que, según las últimas revisiones históricas, ha pasado a ser considerada como la primera computadora programable de la historia, incluso anterior a ENIAC y a otras máquinas estadounidenses.

La vida de Turing fue fascinante pero marcada por la injusticia y la tragedia. Sobre él encontramos innumerables textos especializados en las áreas de matemáticas y computación pero escasos documentos académicos o de divulgación en ciencias sociales. De las fuentes originales sobre las ideas y textos escritos por el propio matemático y relacionados indirectamente con las TIC, nos basamos en: "Intelligent machinery", "Computing machinery and intelligence", diversos

documentos del Kings College de la Universidad de Cambridge, del National Heritage Memorial Fund y que permanecen en Bletchley Park así como en su testamento, todos documentos interesantes y reveladores de la personalidad de Turing, que tuvimos la oportunidad de revisar en el trabajo de campo que realizamos en mayo-junio de 2018 en el Reino Unido y que enriquecieron este trabajo de investigación.

Después de haber ubicado a nuestros personajes en su contexto (espacial y temporal), en las TIC y la criptografía computacional (Capítulos I al III), en el capítulo IV retomamos el artículo de Turing, publicado en 1950 en la revista de filosofía *Mind,* titulado "Maquinaria computacional e inteligencia", que propone situar la pregunta sobre la inteligencia mecánica en una versión del *juego de imitación*, lo que se conoce ahora como *Prueba de Turing*. Con la académica y estudiosa de la lógica matemática Atocha Aliseda, comprobamos que esa *prueba* se considera un pilar para plantear la analogía "la mente es como una computadora", que sirvió de puente entre la filosofía de la mente y la inteligencia artificial. La primera proporcionó la base conceptual; la segunda, las herramientas para representar y manipular el conocimiento. (Aliseda Llera, 2013,10-17).

Por otra parte, pudimos visualizar cómo, del otro lado del Atlántico, en 1948, con su artículo "Teoría matemática de la comunicación", Claude Elwood Shannon demostraba que la información podía definirse y medirse desde el punto de vista científico por medio de *dígitos binarios*[182]. Pudimos entender cómo nació la Teoría de la información, que hoy tiene diversas aplicaciones en todas las áreas del conocimiento y en nuestra vida cotidiana. Pudimos constatar que su interés se centró en aspectos matemáticos (más técnicos), pero también que hizo contribuciones a campos como la criptografía, la computación y la inteligencia artificial: a las TIC.

Basamos el análisis específico de la vida y obra de Shannon también en sus principales biógrafos y textos, particularmente en su *Teoría de la criptografía* y la *Teoría matemática de la información*, concebidas entre 1948 y 1949. Pudimos constatar que la obra criptográfica que Shannon, escrita durante y después de la guerra, se desclasificó sólo años después[183] y por ello fue desconocida por los teóricos de la época.

Con respecto a las TIC fue enriquecedor ubicar su historia y desarrollo, así como enmarcarlas en el contexto sociohistórico de la comunicación secreta, la criptografía computacional y las aportaciones de nuestros personajes. Sobre las TIC encontramos una extensa bibliografía desde la computación, las matemáticas y la historia general de la comunicación como puntos de partida para encontrar los nexos entre los trabajos tanto de Turing como de Shannon.

El capítulo III se centró en los principales modelos y escuelas de las ciencias de la comunicación y la omisión de la comunicación secreta y de la criptografía computacional y de Turing y de Shannon en ellos. Si bien nuestro recorrido fue parcial, lo hicimos sólo en función de proporcionar un panorama general de las teorías de la comunicación que podrían haber se acercado a la comunicación secreta y a la criptografía computacional. Aquí resultó particularmente complejo definir cuáles modelos y teorías incluir pero lo hicimos finalmente con base en las tres corrientes básicas de la comunicación: el funcionalismo, el estructuralismo y la corriente crítica. Sin profundizar, dado que no era el objetivo de este trabajo, de todas el las retomamos a sus principales exponentes y decidimos tomar como puntos de partida a teóricos como Martín Serrano y Karam, no por ser necesariamente los más completos, sino por su capacidad de síntesis, idonea para los fines de este trabajo.

[183] Recordemos que Warren Weaver (1894-1978) tuvo gran importancia para la culminación y el asentamiento de la Teoría Matemática de la Comunicación de 1949, hoy conocida por todos como la Teoría de la Información. Weaver enriqueció el planteamiento inicial de Shannon, que se restringía al ámbito de los lenguajes máquina, y la consecuente transmisión de estos mensajes. A estos dos autores se les debe el esquema lineal de la comunicación: *Fuente/codificador/mensaje-canal/descodificador/destino*.

Seguimos en el capítulo IV con la descripción de las TIC y posteriormente en el Capítulo V con la criptografía computacional y la comunicación secreta. Para ubicar la historia y el desarrollo de la criptografía nos basamos en autores como Martin Gardner, y en David Kahn en cuanto a definiciones sobre cifra, código y mensajes secretos y su exhaustivo análisis de la historia de la criptografía, del antiguo Egipto a los años sesenta del siglo XX y a la batalla de los criptoanalistas Aliados contra las potencias del Eje durante la Segunda Guerra Mundial. De Daniel Martín Reina (2009), David Newton, B.J. Copeland y Simon Singh sus recorridos conceptuales e históricos por la criptografía y la ciencia de los mensajes secretos. También de Marian Rejewski (1981) y Robert Harris, el papel de los polacos y Enigma. La batalla desde Bletchley Park con el ejército y la marina alemanas fue apasionante y tratamos de narrarla de la manera más completa posible e incluyendo a sus principales protagonistas.

Otro eje central de esta investigación fue la comunicación secreta como fenómeno comunicativo, resultado y objeto de la criptografía computacional. Ahí ubicamos las aportaciones del matemático británico y del ingeniero estadounidense en lo referente a la *comunicación secreta*, entendida ésta como un fenómeno comunicativo producto de una práctica social. (Gallego Dueñas, 2012). Para lograrlo, insistimos, partimos del secreto como una forma de relacionarnos los seres humanos "…en la que un actor o actores, en una determinada situación, evitan, limitan o modifican la comunicación de algo (acción, pensamiento, sentimiento…) a otro actor o actores, durante cierto tiempo, haciendo uso de ciertas tácticas, es decir, suponiendo un esfuerzo." (Gallego Dueñas, 2012, 3).

Tomamos en cuenta algunos aspectos lingüísticos y académico Beryl L. Bellman (1981, 1-24), al definir la importancia del lenguaje en el secreto pues mantiene que éste debe ser visto como un método para manejar información oculta en un contexto determinado, con un contexto de significado. Así, un secreto, para serlo, debe tratar sobre una información relevante. Pero, como explica Gallego Dueñas, no es una cualidad de la información sino del modo en

que dicha información se transmite.

Dado que la criptografía consiste precisamente en la transmisión de un lenguaje secreto y que su método es el cifrado, analizamos cómo éste enmascara las referencias originales de la lengua por un método de conversión de un algoritmo que permita el proceso inverso o cifrado y cuyo uso posibilita el intercambio de mensajes que sólo pueden ser entendidos por los destinatarios que poseen la clave. Esta última basada en un *libro de códigos.*

Específicamente en el tema de nuestro interés, es decir, la criptografía en los lenguajes secretos, con Gallego Dueñas pusimos de manifiesto que a través de la criptografía no sólo se oculta el mensaje, sino también se oculta la cifra, la clave de su entendimiento y que una de las técnicas más importantes conceptualmente es el *secret sharing.*[184] Como lo vimos, ese método consiste en la distribución de un mensaje entre un grupo de participantes, cada uno de los cuales tiene una parte. El mensaje sólo puede reconstruirse cuando se combinan un número suficiente de partes pues solas carecen de utilidad. Así, en esta investigación tratamos al secreto no sólo como una forma de comunicar, sino como una manera que despierta el deseo de conocimiento, y que debemos integrar formalmente hoy más que nunca a los estudios de comunicación, reconociendo cabalmente las aportaciones de Turing y de Shannon a su desarrollo.

Y, reiteramos, después de finalizar esta investigación estamos más convencidos que antes de que tanto la criptografía computacional como la comunicación secreta son áreas de estudio indispensables para comprender a profundidad los procesos comunicativos y de interacción social que vivimos en el mundo actual.

[184] Véase también Gómez (2010) y Cascudo (2010). Simplemente recordemos el *hackeo* de los sistemas de inteligencia y más recientemente de los sistemas bancarios y de salud en Gran Bretaña y países en el mundo el 12 de mayo de 2016. Véase la rueda de medios "Ciberataque Masivo por el virus informático WannaCry", donde especialistas de la UNAM y expertos de su Dirección General de Cómputo Académico (DGTIC-UNAM) explicaron que se trató de un ranaware o software para encriptar información ocurrida por carecer de parches de seguridad (actualizaciones) para corregir esa vulnerabilidad. En *Gaceta UNAM* 18 de mayo de 2017, p. 9.

Por ello sostenemos, más que nunca, que tanto la criptografía computacional como la comunicación secreta deben incorporarse a nuestros planes de estudio y proyectos de investigación en las ciencias de la comunicación pues sus productos más inmediatos –las TIC, la computación y el lenguaje digital– forman hoy parte indisoluble de nuestra vida cotidiana, académica y profesional y tanto Alan Mathison Turing como Claude Elwood Shannon fueron fundamentales en sus orígenes y desarrollo y deben ser reconocidos y estudiados con mayor profundidad desde las ciencias sociales y de la comunicación. Hacerlo no sólo como asignaturas obligadas en los programas académicos sino como campos de análisis sumamente prometedores y fascinantes que estamos seguros enriquecerán enormemente el estudio y entendimiento de las ciencias de la comunicación.

GLOSARIO CRIPTOGRÁFICO[185]

A

Álgebra booleana. En informática y matemáticas se trata de una estructura algebraica que esquematiza las operaciones lógicas. Se aplica de forma generalizada en el ámbito del diseño electrónico. Shannon fue el primero en aplicarla en el diseño de circuitos de conmutación eléctrica biestables, en 1948. Esta lógica se puede aplicar al análisis porque es una forma concreta de describir cómo funcionan los circuitos y al diseño ya que teniendo una función aplicamos dicha álgebra, para poder desarrollar una implementación de la función.

Algoritmia. Área que estudia los algoritmos.

Algoritmo. Del griego y latín, *dixit algorithmus.* En matemáticas, lógica y ciencias de la computación es un conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite llevar a cabo una actividad mediante pasos sucesivos que no generen dudas a quien deba hacer dicha actividad.

Algoritmo de cifrado. Método para convertir un texto llano en uno cifrado.

Autoridad certificadora. Entidad (compañía) que es reconocida para poder certificar la asociación de una clave pública a una persona o servidor.

Autenticidad. En computación, estar seguros de la identidad de una entidad ya sea mensaje, persona, servidor, etc.

[185]Basado en Kahn (1967, 1996, 2005), Ángel (s.f.), Martín Reina (2003, 2009), Garrido, Manuel (s.f.) Wikipedia y otros textos digitales.

B

Bit. Contracción de *binary digit* (bajo sugerencia de John W. Turkey, colega de Shannon en los Laboratorios Bell), como la unidad de información y el elemento fundamental de la comunicación.

Bit binario. Según el blog Tecnología Informática (wordpress.com/2007/04/18 "Un Dígito Binario, también conocido como Bit (acrónimo del inglés Binary Digit), es la unidad mínima de almacenamiento o información aplicado en la informática. Un Dígito Binario está representado por un 0 o un 1, que también ambos constituyen el sistema de numeración binario, usando estos dos valores, 0 y 1 (ej., en decimal se usan 10 valores del 0 al 9).Técnicamente tiene varias implementaciones, el 0 y 1 se pueden representar como diferentes valores, donde 0 representaría a un falso o apagado, y el 1, un verdadero o encendido.

C

Certificado digital. Físicamente es un archivo de hasta 2 K de tamaño, que contiene principalmente los datos de una entidad, persona o servidor, la clave pública de esa entidad y la firma de una autoridad certificadora reconocida para poder comprobar la identidad de la persona (o servidor) y valida la clave pública que es asociada a la entidad.

Cifra. Método para ocultar el significado de un mensaje alterando las letras que lo componen.

Cifrado nulo. Técnica es teganográfica o forma de comunicación secreta que oculta la existencia de un mensaje (excepto para su destinatario) consistente en camuflar las letras o palabras del mensaje auténtico dentro de un texto

Cifrador de bloque. Sistema criptográfico que cifra de bloques en bloques, usualmente cada bloque es de 128 bits. Algunos sistemas conocidos son TDES, RC5, AES.

Cifrador de flujo. Sistema criptográfico de cifra de bit en bit, los más conocidos son RC4, SEAL, WAKE.

Cifrar. Acción que produce un texto cifrado (ilegible) a partir de un texto original.

Clave. Conjunto de reglas que establecen con exactitud la manera en que un texto llano se transforma en uno cifrado y viceversa.

Clave privada. Clave secreta que se usa en la criptografía asimétrica.

Clave pública. Clave públicamente conocida, que se usa en la criptografía asimétrica

Clave asimétrica o de clave pública. Usa una clave pública y una clave privada para realizar el cifrado y el descifrado. Las claves son distintas pero están relacionadas matemáticamente. Generalmente, la clave privada se mantiene en secreto y se usa para cifrar datos, mientras que la clave pública se distribuye a las partes interesadas y se usa para descifrar datos. La criptografía asimétrica también se usa para firmar datos.

Clave simétrica. Clave secreta que tienen ambos lados de una comunicación. En la criptografía simétrica o de clave secreta se usa una misma clave para cifrar y descifrar mensajes en el emisor y el receptor. Las dos partes deben ponerse de acuerdo sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.

Código. Conjunto de reglas por las que una palabra o frase es representada por otra palabra o símbolo.

Códigos (libro). Libro de recopilación del significado de las palabras codificadas.

Códigos binarios. Sistemas numéricos usados para la representación de textos o procesadores de instrucciones de computadora, utilizando el sistema binario (sistema numérico de dos dígitos, o *bit*: el "0" /cerrado/ y el "1" /abierto/). En informática se usan con variados métodos de codificación de datos, tales como cadenas de caracteres, o cadenas de bits.

Compartición de secretos. Esquema criptográfico que tiene como entrada un secreto (por ejemplo una clave criptográfica) y como salida un numero de partes del secreto y todas o algunas de estas partes sirven para reconstruir el secreto.

Computabilidad. Parte de la computación que estudia los problemas de decisión, que pueden ser resueltos con un algoritmo o equivalente con la llamada máquina de Turing. La teoría de la computabilidad se basa en tratar de responder los problemas que pueden resolver una máquina de Turing u otras máquinas.

Criptografía. Conjunto de técnicas (entre algoritmos y métodos matemáticos) que resuelven los problemas de autenticidad, privacidad, integridad y no rechazo en la transmisión de la información. Conjunto de técnicas, que originalmente tratan sobre la protección o el ocultamiento de la información frente a observadores no autorizados. Entre las disciplinas que engloba cabe destacar la Teoría de la Información, la Complejidad Algorítmica y la Teoría de números o Matemática Discreta, que estudia las propiedades de los números enteros. A través de la criptografía la información puede ser protegida contra el acceso no autorizado, su interceptación, su modificación y la inserción de información extra. También puede ser usada para prevenir el acceso y uso no autorizado de los recursos de una red o sistema informático y para prevenir a los usuarios la denegación de los servicios

a los que sí están permitidos. Hoy es la metodología para proveer la seguridad de las redes telemáticas, incluyendo la identificación de entidades y autenticación, el control de acceso a los recursos, la confidencialidad de los mensajes transmitidos, la integridad de los mensajes y su no repudio.

Criptografía asimétrica. Conjunto de métodos que permite establecer comunicación cifrada, donde una de las claves es pública y la otra clave es privada (secreta). Cada usuario tiene un par de claves, una pública y otra privada.

Criptografía simétrica. Conjunto de métodos que permite establecer comunicación cifrada, con la propiedad de que ambos lados de la comunicación tienen la misma clave, y ésta es secreta.

Criptografía visual. Esquema de compartición de secretos donde el secreto es una imagen y las partes son también imágenes.

D

Decisión. Problema de la (Entscheidungsproblem), al problema de hallar un método de cálculo que permita decidir mecánicamente para toda fórmula lógica si es o no válida. Una respuesta afirmativa a este problema podría implicar que todo problema matemático fuese mecánicamente resoluble. Según definiciones sencillas; propiedad de los sistemas formales cuando, para cualquier fórmula en el lenguaje del sistema, existe un método efectivo para determinar si esa fórmula pertenece o no al conjunto de las verdades del sistema. Cuando una fórmula no puede ser probada verdadera ni falsa, se dice que la fórmula es *independiente*, y que por lo tanto el sistema es *no decidible*.

Descifrar. Acción inversa de cifrar, es decir, convierte un texto cifrado a otro legible (texto original). Obtener a partir de un algoritmo de cifrado y la clave utilizada, el mensaje llano de un mensaje cifrado.

Dígitos binarios. En el mundo de los ordenadores dígito binario se suele abreviar con la palabra "bit".

E

Eficiencia (límite). Propiedad que con la redundancia es fundamental para transmitir información en la telefonía, la radio, la televisión, la telegrafía, etc.

Enigma (máquina). Dispositivo electromecánico (combinación de partes mecánicas y eléctricas) constituido fundamentalmente por un teclado similar al de las máquinas de escribir cuyas teclas eran interruptores eléctricos, un engranaje mecánico y un panel de luces con las letras del alfabeto. Estaban provistas de una batería que encendía una lámpara de un a serie de ellas, que representan cada una de las diferentes letras del alfabeto. La parte mecánica y constaba de varios rotores conectados entre sí. Cada rotor era un disco circular plano con 26 contactos eléctricos en cada cara, uno por cada letra del alfabeto. Cada contacto de una cara estaba conectado o cableado a un contacto diferente de la cara contraria. Cada uno de los cinco rotores proporcionados con la máquina Enigma estaba cableado de una forma diferente y los rotores utilizados por el ejército alemán poseían un cableado distinto al de los modelos comerciales.

Entropía. Energía que no es utilizable ante el advenimiento de un proceso termodinámico; aquella energía que no es utilizada y que por tanto no es considerada útil para tal proceso. En la termodinámica (o rama de la física que estudia los procesos que surgen a partir del calentamiento de energías y de la puesta en movimiento de diferentes elementos naturales), la entropía figura como la referencia o la demostración de que cuando algo no es

controlado puede transformarse y desordenarse. La entropía, además, supone que de ese caos o desorden existente en un sistema surja una situación de equilibrio u homogeneidad que, a pesar de ser diferente a la condición inicial, suponga que las partes se hallan ahora igualadas o equilibradas.

F

Familia criptográfica. Conjunto de sistemas criptográficos que basan su seguridad en el mismo problema matemático, actualmente las familias criptográficas más conocidas son las que basan su seguridad en el Problema de Factorización Entera (RSA, RW), los que la basan en el problema del logaritmo discreto (DH, DSA), y los que la basan en el problema del logaritmo discreto elíptico (DHE, DSAE, MQV).

Fibonacci (secuencia). La sucesión o secuencia de Fibonacci es una sucesión matemática infinita. Consta de una serie de números naturales que se suman de a 2, a partir de 0 y 1 y se realiza sumando siempre los últimos 2 números de la siguiente manera: 0,1,1,2,3,5,8,13,21,34...

Firma digital. Método que usa criptografía asimétrica y permite autenticar una entidad (persona o servidor), tiene una función igual que la firma convencional. Consiste en dos procesos, uno de firma y otro de verificación de la firma. Físicamente es una cadena de caracteres que se adjunta al documento.

H

Hardware. Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Hipercomputación. Lo que queda detrás de la computación, es decir, la computación de algo no computable por una máquina de Turing. La teoría de la hipercomputación rechaza la idea de un a computabilidad absoluta, independiente de cualquier teoría lógica, matemática, física o biológica subyacente. Para implementar un hipercomputador, se requerirían modelos fundamentados en la física y la computación cuántica.

I

Inteligencia artificial. Programa de computación diseñado para realizar determinadas operaciones que se consideran propias de la inteligencia humana, como el autoaprendizaje.

Interfaz. En informática se usa para nombrar a la conexión funcional entre dos sistemas, programas, dispositivos o componentes, que proporciona una comunicación de distintos niveles permitiendo el intercambio de información. Algunos ejemplos son interfaces de usuario (entre computadora y persona) como sería una pantalla o un ratón (si hablamos de *hardware*) o la ventana gráfica de un programa con la que interactuamos (si hablamos de *software*); las interfaces físicas (entre dos dispositivos) como el SCSI o el USB; o las interfaces lógicas (entre dos programas) como la API o el DOM.

L

Logaritmos. Nos dicen cómo multiplicar números sumando, en su lugar, números que están relacionados. Es importante porque sumar es mucho más simple que multiplicar.

Longitud de la clave. Número de bits (ceros y unos) que tienen las claves y es solo uno de los parámetros de los que depende la seguridad de un sistema

criptográfico. Actualmente se usan 128 para las claves simétricas, 1024 para el sistema asimétrico RSA, 163 para los sistemas asimétricos que usan curvas elípticas.

M

Máquina de Turing. Tipo de máquinas abstractas de estructura conceptualmente muy simple, capaces de realizar complejas funciones de computación.

N

Números "grandes". Si tiene longitud al menos de 512 bits (155 dígitos), a causa de que los procesadores actuales manejan solo números de 32 bits.

Número primo. Número entero que no tiene divisores diferentes a 1 y a sí mismo, por ejemplo 2,3,5,7,11.

P

Par de claves. Una clave privada y otra pública, usadas en la criptografía asimétrica.

Primitiva criptográfica. Función más básica que compone un sistema criptográfico; existen la primitiva de cifrado, la primitiva de descifrado, la primitiva de firma, la primitiva de verificación de firma, etc.

Privacidad. En informática, control en el acceso de la información y sólo permitido a personas autorizadas.

Problema de Factorización. Problema inverso a la multiplicación, es decir el problema de encontrar los factores conocidos el producto. En criptografía los

números a factorizar son los productos de dos números primos de la misma longitud, el producto tiene al menos 768 bits.

Programa informático o programa de computadora. Secuencia de instrucciones escritas para realizar una tarea específica en una computadora. Este dispositivo requiere programas para funcionar, por lo general, ejecutando las instrucciones del programa en un procesador central.

Protocolo (criptográfico). Parte más visible de la aplicación; está compuesto de esquemas criptográficos conjuntamente con otras operaciones que permiten proporcionar seguridad a una aplicación más específica.

Prueba de Turing o test de Turing. Consiste en una prueba de la habilidad de una máquina para exhibir un comportamiento inteligente similar al de un ser humano o indistinguible de éste.

R

Relevadores o relés. Inventado por Joseph Henry en 1835, es un dispositivo electromagnético que funciona como un interruptor controlado por un circuito eléctrico en el que, por medio de una bobina y un electroimán, se acciona uno o varios contactos que permiten abrir o cerrar otros circuitos eléctricos independientes. Dado que puede controlar un circuito de salida de mayor potencia que el de entrada, se considera como un amplificador eléctrico. Así se emplearon en telegrafía como repetidores que generaban una nueva señal con corriente procedente de pilas locales a partir de la señal débil recibida por la línea.

Rizos. En criptografía, cadenas que enlazaban letras de un texto cifrado.

S

Software. Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

T

Teorema. Proposición que afirma una verdad demostrable. En matemáticas, es toda proposición que partiendo de un supuesto (hipótesis), afirma una racionabilidad (tesis) no evidente por sí misma. También es una fórmula bien formada que puede ser demostrada dentro de un sistema formal, partiendo de axiomas u otros teoremas. Demostrar teoremas es un asunto central en la lógica matemática. Los teoremas también pueden ser expresados en lenguaje natural formalizado. Los teoremas generalmente poseen un número de premisas que deben ser enumeradas o aclaradas de antemano. La conclusión del teorema es una afirmación lógica o matemática que es verdadera bajo las condiciones dadas. Su contenido es la relación que existe entre las hipótesis y la tesis o la conclusión.

Teoría de la información. Define cuánta información contiene un mensaje, en términos de las probabilidades con las que los símbolos que lo componen tienen la posibilidad de darse. Marca el comienzo de la era de la información. Estableció los límites en la eficiencia de las comunicaciones, permitiendo a los ingenieros dejar de buscar códigos que fuesen demasiado efectivos para existir. Es básica en las comunicaciones digitales de hoy. Provocó códigos eficientes de detección y corrección de errores, usados en todo, de CDs a sondas espaciales. Las aplicaciones incluyen estadística, inteligencia artificial, criptografía y obtener significado de la secuencia de ADN. (Stewart, 2015).

Texto cifrado: documento que ha sido cifrado a partir de un texto original.

Texto original: documento inicial, antes de ser cifrado.

BIBLIOGRAFÍA

A

ACM. (2014). "Tecnologías de la Información", *Computing Carrers and Degrees*, Association for Computing Machinery.

Agar, Jon, (2001). *Turing and the Universal Machine* (Icon).

Aguirre Rojas, Carlos Antonio (2004). *La historiografía en el siglo xx. Historia e historiadores*, Barcelona: Montesinos.

Aliseda Llera, Atocha (2007). " Emerge una nueva disciplina, las ciencias cognitivas. Ciencias 88, oct.-dic. 23-31, México: UNAM

——— (2013). ¿Inteligencia mecánica? La pregunta de Alan Turing, *Ciencia. Revista de la Academia Mexicana de Ciencias*, 64 (4) 10-17.

Alter, Steven (2008). *Defining Information Systems as Work Systems: Implications for the IS Field,* San Francisco: University of San Francisco.

Ángel Ángel, José de Jesús, (s. f.) Recuperado en noviembre de 2018 de www.softdownload.com.ar.

Alva de la Selva, A. R. (2015). *Telecomunicaciones y TIC en México*, México: UNAM/Comunicación Social.

Álvarez Debans, Norberto, (s. f.), ADN en 21:17.

Amoroso, E. (1994). *Fundamentals of Computer Security Technology*, USA: Prentice Hall Inc.

Annan, Koofi (2003). Discurso inaugural, WSIS, Ginebra.

Atiar Rahman (2009). *Conceptos fundamentales y lista*. Recuperado en septiembre de 2018 de stretdirectory.com.

Armesto, Constantino (1995). *Por los senderos de la ciencia*, Madrid: Celeste Ediciones.

B

Basil H. Liddell y Hart Caral (2009). *Historia de la Segunda Guerra Mundial*, México: Edit. Noguer.

Bauer, Friedrich Ludwig (2000). *Decrypted Secrets: Methods and Maxims of Cryptology*, Alemania: Springer-Verlag Telos.

Becerra, M artín (2002). *Sociedad de la Información: proyecto, convergencia, divergencia*, Buenos Aires: Editorial Norma.

Bellman, Beryl L. (1981). The Paradox of Secrecy. *Human Studies* (4): 1-24.

——— (1984). *The Language of Secrecy. Symbols & Metaphors in Poro Ritual*. New Brunswick. New Jersey: Rutgers University Press.

Black, E dwin. 1992. *Rhetorical Questions*. Ch icago-London: T he U niversity of Chicago Press.

Berlo, David K.(1960), *El proceso de la comunicación*.

Bletchley Park (2018). *Home to the Codebreakers,* Guidebook, L ondon: English Heritage.

Brennan, R. E. (1969). *Historia de la psicología*, Madrid: ed. Madrid,

Bloch, M arc (1996). *Apología para la historia o el oficio del historiador*, México: FCE.

Boden, M.A. (1977). *Inteligencia artificial y hombre natural,* Madrid*: Tecnos*.

Bologna, J . y Walsh, A. M . (1997). The A ccountant´s Handbook of Information Technology (1): John Wiley and Sons.

Braudel, Fernand (1991). *Escritos sobre historia*, México: FCE.

C

Cascudo Pueyo, I gnacio (2010). On A symptotically G ood S trongly M ultiplicative Linear S ecret S haring. Tesis D octoral pr esentada e n el Departamento de Matemáticas, Oviedo, España: Universidad de Oviedo.

Castells, M anuel (1999). *La era de la información, Economía, sociedad y cultura*, 1, México: Siglo XXI.

Casti, John L. (1998). *El Quinteto de Cambridge*, Madrid: Taurus Pensamiento.

Christensen, C hris (2007). Polish m athematicians f inding p atterns i n E nigma messages, *Mathematics Magazine*, 80(4) 247-273.

Ciencia, revista de la AMC sobre Alan Turing y la computación (oct-dic. de 2013): Vol. 64, México.

Creative Commons (s.f.) “Diez momentos en la historia de las TIC”, B Y NC-SA

Copeland, J. y D. Proudfoot (1999). Alan Turing s forgotten ideas in computer science, *Scientific American*, 280 (4):99-103.

——— (2004). *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life plus Secrets of Enigma*, Oxford: Oxford University Press.

——— (2005). *Alan Turing's Automatic Computing Engine: The Master Codebreaker's Struggle to Build the Modern Computer,* Oxford: Oxford University Press.

——— (2006). *Colossus: the Secrets of Bletchley Park s Code-Breaking Computers*, Oxford University Press, Oxford.

Cora Diamond ed. (1976). *Wittgenstein's Lectures on the Foundations of Mathematics*, Sussex, England: The Harvester Press.

Couétoux, Michel et al (1998). *Figures du secret,* 129-206, Grenoble: Presses Universitaires.

D

Davis, Martin (2000). Engines of *Logic Mathematicians and the Origins of the Computer*, London: Norton.

Davis, Martin (2000). *The Universal computer: the Road from Leibnitz to Turing*, W.W. :Norton & Company.

D'Adamo, Orlando J. (2007). *Medios de Comunicación y Opinión Pública*, México: McGraw-Hill Interamericana.

Deavours, Cipher, A. (1985). *Machine Cryptography and Modern Cryptanalysis*, UK: Artech House Inc.

Debrosse, Jim, Colin Burke (2004). *The Secret in Building 26: The Untold Story of America's Ultra War against the U-boat Enigma Codes*.

Deleuze, Gilles y Guattari, Félix (2006). Mil mesetas, *Pretextos,* Valencia: univeerisdad de Valencia.

De Sola Pool, Ithiel (1993). *Tecnología sin fronteras. De las telecomunicaciones a la época de la globalización*, México: FCE.

Díaz Maldonado, Rodrigo, (2001). El discurso histórico, *Fractal* 23, VI, 39-58.

"Diez momentos clave en la historia de las TIC", publicados en *Creative Commons BY NC-SA*.

Diffie, W., M.E. Hellman (1976). *New Directions in Cryptography, Transactions on Information Theory*, IT22 (6), 644-654.

Dilthey, Wilhelm *Selected Works* (2010), Vols. I *Introduction to the Human Sciences* y IV *Hermeneutics and the Study of History* USA: Princeton University Press.

Dimitris, N., Chorafas (1965). *System and Simulation*, EUA: Academic Press.

Dysson*, George: (2016). La catedral de Turing*, Barcelona, España: Paidós.

E

Eco, Umberto (1995). *Interpretación y sobreinterpretación*, Cambridge, U. K: Cambridge University Press.

——— (2001). *La Estructura ausente,* Barcelona: Lumen.

Elias, Norbert (1989). *El proceso de civilización*, México: FCE.

——— (1999): *Los alemanes*, México: Instituto Mora.

Evolución Tecnológica (2009).

F

Fabbri, Paolo (2001). *Tácticas de los signos*. Barcelona: Gedisa.

Ferrer, Eulalio (2001). *Comunicación e Información*. México: FCE.

Fernández González, Sandra (2009). *¿Qué son las nuevas tecnologías?*, México.

Ferraris, Maurizio (1999). *La hermenéutica*, México: Taurus.

——— (2002). *Historia de la hermenéutica*, Siglo XXI, México.

Flores Morador, Fernando (2003). Lo humano y lo artificial en la comunicación electrónica, *El Catoblepas*, Revista crítica del presente (12), México.

Focardi, R., R. Gorrieri (1995). A classification of security properties, *Journal of Computer Security,* 3 (1).

Foulquie, P. (1959). *La psychologie contemporaine*. París.

Friedman, W. (1967). Cryptology, *Encyclopedia Britannica*, 6, 844-851.

Fuentes Navarro, Raúl (coord.) (2004): *Producción, circulación y reproducción académicas en el campo de la comunicación en México*. Guadalajara, México: ITESO.

G

Gadamer, Hans-Georg (1966). *Verdad y método,* Salamanca: Sígueme.

Galbraith, Steven D. (2012): *The Mathematics of Public Key Cryptography*, U.K., England: Cambridge University Press.

Galindo, Jesús (2002). *Notas para una comunicología posible. Elementos para una matriz y un programa de configuración conceptual-teórica*. Disponible en la página del autor. http://www.geocities.com/arewara/arewara.htm.

Gallego Dueñas, Francisco J. (2001). Gramática del secreto, *Sociolingüística y secreto*, Universidad Nacional de Educación a Distancia, Manuscrito, UNED.

——— 2012. Introducción a una teoría para una (micro) sociología del secreto. Tesis Doctoral inédita, UNED.

Gangemi, G.T., D. Russell (1991). *Computer Security Basic*: O'Reilly.

Garrido, Manuel (s.f.) *Lógica simbólica,* Madrid: Técnos.

Garrido, Manuel y otros (2005). *El legado filosófico y científico del siglo XX,* Madrid: Tecnos.

Givierge, M., "*Cours de Cryptographie*" (2018). Recuperado en mayo del 2018 en mrs.fr/~andreea.dragut/enseignementCLAA/presCryptBlowfish.pdf.

Goldstine, Herman H. (1972). *The Computer from Pascal to von Neumann*, Princeton, NJ: Princeton University Press.

Gómez, Joan (2010). *Matemáticos, espías y piratas informáticos*. *Codificación y criptografía.* Barcelona: RBA.

Grondin, J. (2008). *¿Qué es la hermenéutica?,* Barcelona: Herder.

Guillén Torres, Beatriz (2016). " El verdadero padre de la I.A", Ventana del conocimiento.

H

Habermas, Jurgen (1981). *Teoría de la acción comunicativa*, Madrid: Taurus.

——— (2015). *Mundo de la vida, política y religión*, Madrid: Trotta.

Hankerson, D arrel, A lfred J . M enezes, S cott Vanstone (2010). *Guide to Elliptic Curve Cryptography*: Springer.

Hartley, R alph V. L. (1928). Transmission o f I nformation, *Bell System Technical Journal* 7: 535–563.

Heidegger, Martin (1951). *Ser y Tiempo,* México: FCE.

Hernández, Pablo María (1996). *Filosofía de hoy*, Universidad Autónoma de Santo Domingo: Editora Impresos Goris.

Hernández Quiroz y Sergio Rajsbaum, editores huéspedes (2014). Alan Turing y la computación, *Ciencia, revista de la Academia Mexicana de Ciencias*, México: AMC

Herrera Restrepo, Daniel (1986). *Escritos sobre fenomenología*, Bogotá: Biblioteca Colombiana de Filosofía.

Hinsley, F .H. (2001). *Codebreakers: The Inside Story of Bletchley Park*, U nited Kingdom: BP

Hobsbawm, E ric (1994). *Historia del siglo XX*, B uenos Aires: E dit. Critica, G rijalbo Mondadori.

Hodges, Andrew, (1983). *Alan Turing: the Enigma*, London: Burnett Books Ltd.

——— (1997)*: A Natural Philosopher*, the Great Philosophers Series, London: PUP.

——— (2012). *Alan Turing: the Enigma.* The C entenary E dition: Princeton University Press.

Hoffstein, J effrey, J ill P ipher, J .H. S ilverman (2008). *An Introduction to Mathematical Cryptography*: Springer.

Horgan, J ohn (1990). “ Claude E . S hannon: U nicyclist, J uggler and F ather o f Information Theory.” *Scientific American* 242: 20–22B.

I

Igarza, R oberto (2008). *Nuevos medios. Estrategias de convergencia*, Buenos Aires: La crujía.

J

Jacob, O. (1998). *La science du secret*, París: Éd.Odile.

Jagjit, Sinah, (1976). *Teoría de la información, del lenguaje y de la cibernética*, México: Alianza edit.

K

Kahn, David (1967). *The codebreakers*, New York: Macmillan.

——— (1996). *The codebreakers: the comprehensive history of secret communication from ancient times to the Internet*.

——— (2005). *The german Enigma cipher machine: beginnings, success, and ultimate failure*.

Karam, Tanus (2005). " Una introducción al estudio de la epistemología de la comunicación desde la obra de Manuel Martín Serrano", *Cinta de Moebio*, Revista de Epistemología de Ciencias Sociales, México.

Koblitz, Neal (1994). *A Course in Number Theory and Cryptography*: Springer.

Kozaczuk, Wladyslaw y Wadysaw Kozaczuk, Jerzy Straszak (2004). *Enigma: How the Poles Broke the Nazi Code.*

L

Lahoz-Beltrá (2005). *Del primer ordenador a la inteligencia artificial.* Madrid: Nivola libros.

Lavington, Simon (2016). *Alan Turing and his contemporaries. Building the world's first computers*, BISL, Chippenham, UK: The Chartered Institute for IT.

Leavitt, David (2006). *The man who knew too much: Alan Turing and the invention of the computer*, great discoveries, W.W: Norton & Company.

Levy, Steven (2002). *Cómo los informáticos libertarios vencieron al gobierno y salvaguardaron la intimidad en la era digital*, Madrid: Alianza.

Lidl, R., H. Niederreiter (1983). *Encyclopedia of Mathematics and Its Applications* Vol. 20, USA: Addison Wesley.

Lister, Martin (2009). *New Media. A critical introduction,* London & New York: Routledge.

Lince Campillo, Rosa Ma. y Julio Amador Bech (Coord.), (2012). *Horizontes de interpretación. La Hermenéutica y las ciencias humanas,* México: UNAM.

Luhmann, Niklas, (1983). *Teoría de la sociedad,* México: UIA-U de G-ITESO.

——— (1984). *Sistemas sociales*, Barcelona- México: Anthropos-UIA-CEJA.

M

MacManus, Richard (2008). “Top Health 2.0 Web Apps”.

Maggio Mariana (2012). “Enriquecer la enseñanza”. Cap. 4 “Los nuevos entornos y su enseñanza”, Buenos Aires: Paidós.

Malbernat, Luc ía R osario (2010). Tecnologías educ ativas e i nnovación en l a Universidad. Recuperado enmarzo 2018 en LaCapitalmdp.com.

Manovich, Lev (2005). *El lenguaje de los nuevos medios de comunicación. La imagen en la era digital*, 163, Barcelona: Paidós Comunicación.

Marc, E dmond y P icard Dominique (1992). *La interacción social. Cultura, Instituciones y comunicación*, Barcelona: Paidos.

Markus y Daniel Robey. “TIC y cambios organizativos” en blog de autores.

Martínez López (2009). “Sistemas d e P ago S eguro. S eguridad en el C omercio Electrónico”, España: Universidad de Jaén.

Martínez N avarro, G ermán (s. f.) “La máquina E nigma y ot ros dispositivos d e encriptación” y http://www.worldlingo.com/ma/enwiki/es/Enigma_machine.

Martín R eina, D aniel (2003): M ensajes s ecretos, *¿Cómo ves?* No. 5 9, México: DGDC-UNAM.

——— (2009). *Criptografía. Un recorrido histórico por la ciencia de los mensajes secretos*, México: Editorial Terracota.

Martín Serrano, Manuel (1977). *La mediación social*, Madrid: AKAL.

——— (1978). *Métodos actuales de investigación social*. AKAL, Madrid.

——— (1982). *Teoría de la Comunicación*, 2ª ed., Madrid: UCM.

——— (1993). *La Producción Social de Comunicación,* Madrid: Alianza/ Universidad, Madrid.

Mattelart, Armand y M ichèle Mattelart (1999). *Historias de las teorías de la comunicación*. Buenos Aires: Paidós.

Maturana, Jesús (01-03-2008). “Ejemplos de miniaturización: Relojes Multimedia”.

Méndez, I gnacio y Pablo G onzález C asanova (1993). *Matemáticas y ciencias*

sociales, México: CEIH-UNAM/Miguel Ángel Porrúa, México.

Menezes, A lfred, Paul v an O orschot y Scott V anstone (1996). *Handbook of Applied Cryptography*, CRC Press.

Molina y V edia, S ilvia (coordinadora) (2009). *Comunicación y sistemas emergentes*, México, UNAM.

Moore, P eter, (2006). *Pequeñas grandes ideas: Ciencia*, B arcelona: Ediciones Oniro.

Murphy, G., (1964). *Introducción histórica a la psicología contemporánea*, Buenos Aires.

N

Norton, Peter (1995). Introducción a la computación, México:Editorial Mc Graw Hill.

O

Odlyzko, A.M. (1 993). *Public Key Cryptography*, A T&T Bell L aboratories, N ew Jersey, USA: Murray Hill.

Ortiz, Bruno (2009). “En solo 40 años internet ha modificado nuestro mundo”

P

Paar, C hristof, J an P elzl, B art P reneel (2010). *Understanding cryptography: a textbook for students and practitioners*: Springer.

Peña, R icardo, (2012). “¿Computadores v on N eumann, o c omputadores T uring?”, *Año Turing,* 06 de septiembre.

Philip, Rit a (1998). “La t eoría del ac tuar c omunicativo de J ürgen H abermas: un marco para el a nálisis de l as condiciones s ocializadoras e n l as s ociedades modernas”, Radl, Papers, 56.

Prados, J ohn (2001). *Combined fleet decoded: the secret history of american intelligence and the japanese navy in World War II*: US Naval Institute Press.

Preneel B., V. Rijmen (eds.) (1998). *State of the art in applied cryptography*, LNCS 1528.

Price, Robert (1985). A conversation with Claude Shannon: one man’s approach to problem solving.”*Cryptologia* 9: 167–175.

R

Rancière, Jacques (1993). *Los nombres de la historia*, Buenos Aires: Ediciones Nueva Visión.

Reinitz, John (2012) La morfogénesis según Alan Turing (consultado en 2012).

Rejewski, Marian (1981). "How Polish mathematicians broke the Enigma cipher", *IEEE Ann. Hist. Comput*., 3(3):213-234.

Ricoeur, Paul, (1969). *Essais d'herméneutique*, París: Seuil.

——— (1995): "La explicación y la comprensión", en *Teoría de la interpretación. Discurso y excedente de sentido*, México: UIA-Siglo XXI.

Ricœur, Paul, (1995). *Tiempo y narración*, , México: Siglo XXI.

Rizo García, Marta (2004). El camino hacia la nueva comunicación, *revista Razón y palabra,* Nº 40 Agosto/Setiembre.

Rodrigo Alsina, Miquel (1995). Los modelos de la comunicación, Madrid:Tecnos,

Rosenblueth, Arturo, (1970). *Mente y cerebro: una filosofía de la ciencia,* México: Siglo XXI editores y El Colegio Nacional.

S

Sánchez Ruiz, Enrique (2002). "La investigación latinoamericana de la comunicación y su entorno social: notas para una agenda", *Diálogos de la comunicación*, No. 64.

Saussure, F. de (1913). Curso de lingüística general, Paris: éd. Payot,

Schneier, B. (1996). *Applied Cryptography*, U.K.: John Wiley & Sons, Inc.

Schramm, Wilbur (1978). *Nuevas dimensiones en la psicología y la comunicación*. Buenos Aires: Edisar, distribuidora argentina.

Sebag-Montefiore, Hugh (2001). *Enigma: The Battle for the Code*, W&N.

Segal, Jérôme (2003). *Le zéro et le un: histoire de la notion scientifique d'information*. Paris: Syllepse.

Shannon, Claude Elwood (1938). *A symbolic analysis of relay and switching circuits,* Trans. American Institute of Electrical Engineers, USA, Vol. 57 713–723.

——— (1948). "A Mathematical Theory of Communication", *Bell System Technical Journal,* No. 27, 379–423, 623–656.

——— (1949). “Communication theory of secrecy systems”, Bell System Technical Journal, No. 28, 656-715.

——— (1949). “Communication in the Presence of Noise”, *Proceedings of the Institute of Radio Engineers* No. 37: 10–21.

——— (1950). “Programming a Computer for Playing Chess”, *Philosophical Magazine* No. 41, 256–275.

——— (1951). “Prediction and Entropy in Printed English”, *Bell System Technical Journal* No. 30: 50–64.

Simmel, Georges. 1986 (1908). Del secreto y la sociedad secreta. En *Sociología*. Vol. 1. 357-424. Madrid: Alianza.

Simmons, G.J. (2000). “Cryptology”, *The New Encyclopaedia Britannica*, Macropaedia Vol 16.

Singh, Simon (2012). *The code book: the science of secrecy from ancient Egypt to quantum cryptography*, Anchor; Reprint edition.

Sinkov, Abraham (2009). *Elementary cryptanalysis*, USA: Mathematical Association of America.

Sloane, N.J.A.; Wyner, Aaron D. (1993). *Claude Elwood Shannon: Collected papers*. Nueva York: IEEE Press.

Smith, Michael (2011). *The secrets of Station X. How Bletchley Park helped win the war*, London: Biteback Publishing Ltd.

Stewart, Ian (2015). *17 ecuaciones que cambiaron al mundo,* México: Edit. Crítica.

T

Taylor, Richard, A. Rosenblueth y N. Wiener, (1987). *Controversia sobre la intencionalidad del comportamiento,* México: Dirección General de Publicaciones, UNAM, México.

Temas de IyC (Abril/Junio 2012). La ciencia después de Alan Turing, Un monográfico sobre su vida y obra, No. 68, México.

Teuscher, C. (2004). *Alan Turing: life and legacy of a great thinker*: Springer-Verlag.

Thompson, John B. (2003). *Hermeneutics: a study in the thought of Paul Ricoeur and Jürgen Habermas*, Cambridge, UK: Cambridge University Press.

——— (2010): *Ideología y cultura moderna*, México: UAM-X.

Triki, Mo unir. (2002). “ Pragmatics f or E SP P urposes”. *GEMA Online Journal of Language Studies*. Vol.2(1) ISSN1675-802.

Tsybakov, B oris, “Remembering C laude S hannon”. R ecuperado e n http://echo.gmu. edu/shannon/survey/memories.php.

Turing, Alan Mathison (1936-37). “On computable numbers, with an a pplication to the E nstscheidungsproblem, *Proceedings of the London Mathematical Society*, 42:230-265.

——— Escritos en www.itpro.co.uk/631417/turing-papers-saved-for-bletchley, donde pu eden c onsultarse l os es critos de T uring q ue per manecieron s ecretos varias déc adas, y f orman par te d el *National Heritage Memorial Fund* y permanecen en Bletchley Park

——— (1950): “Computing machinery and intelligence”, *Mind*, 59:433-460.

——— (1992). “Intelligent Machinery”, en Ince D.C. editor.

——— *(2012). Collected Works of A.M. Turing-Mechanical Intelligence*, Cambridge: Elsevier.

——— (1992). “Intelligent Machinery”, Collected Works of A.M. Turing-Mechanical Intelligence.

Turing, Sara, (1959). *Alan M. Turing,* Cambridge: Heffer.

——— (2012): *Alan M. Turing,* Centenary Edition, Cambridge, U. K.: University Printing House

U

Unión Internacional de T elecomunicaciones (UIT), (2001). *Manual para la recopilación de datos administrativos de las telecomunicaciones y las TIC,* Ginebra, Suiza.

V

Valdés, M anuel L uis M y Lui s A renas (2005). *El legado filosófico y científico del siglo XX*, Madrid: Ediciones Cátedra

Valek, Gloria (2010). “El legado de un hombre poco común. Arturo Rosenblueth”, en *¿Cómo ves?* 187, México: DGDC-UNAM.

——— (2012). “Alan Mathison Turing. Explorador de límites”, en *¿Cómo ves*? 163, México: DGDC-UNAM.

——— (2016a): “¿Qué leer’?”, Revista *¿Cómo ves?* 215, México: DGDC-UNAM.

——— (2016b): “¿Qué leer?”, en *¿Cómo ves?* 206, México: DGDC-UNAM.

——— (2016c): “ Claude E . S hannon, el g ran i nnovador”, en *¿Cómo ves?* 210, México: DGDC-UNAM.

Van M anen M ax y Levering, Bas (1999). *Los secretos de la infancia. Intimidad, privacidad e identidad*. Barcelona: Paidós.

Verdu, Sergio (1998). “ Fifty Y ears of S hannon Theory.” *IEEE Transactions on Information Theory* 44: 2057–2078.

Von Newman, J. (1958). *The Computer and the Brain*, USA: Yale University Press.

W

Wallerstein, E mmanuel (1996). *Abrir las ciencias sociales. Comisión Gulbenkain para la reestructuración de las ciencias sociales,* México: Siglo XXI.

Watzlawick, P aul *et al (*1966). *Teoría de la Comunicación Humana,* Barcelona: Herder.

Welchman, Gordon (1997). *The hut six story,* London: M&M Baldwin (Editor).

White, Hayden (1992). *El contenido de la forma*, Barcelona: Paidós básica.

Wiener, Norbert (1948). *Cybernetics , or Control and Communication in the Animal and the Machine*. Paris, France: Hermann et Cie.

Willmott, H .P. (2005). *World War II*, R obin C ross & C harles M essenger, D orling Kindersly.

Wilson, D eindre y S perber, D an (2004). “La t eoría de l a r elevancia”. *Revista de investigación Lingüística*. Vol VII: 233-282.

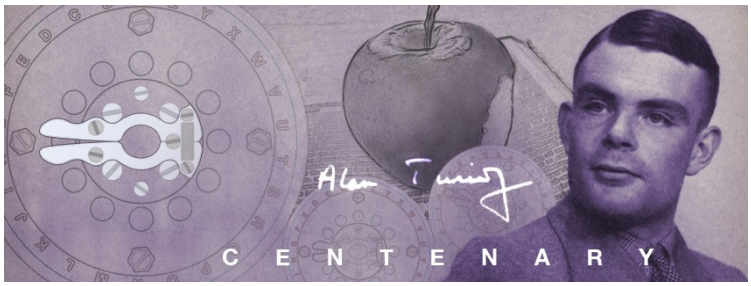
Wolf, M auro (1996). *La investigación de la comunicación de masas*. México: Paidós.

Wyner, A aron, D . y Neil, J . A . S loane e ds., (1993. *Claude Elwood Shannon: Collected Papers*, P iscataway, N J, IE EE P ress. Incluye su t esis de m aestría (http://libraries.mit.edu/) la carta a Vannevar Bush de febrero de 1939 y su tesis de doctorado (http://libraries.mit.edu/). Los t rabajos de m aestría y doctorado también están disponibles en el repositorio institucional del MIT.

Z

Zempléni, A ndras (1976). «La c haîne du s ecret», *Nouvelle Revue de Psychanalyse,* 14, Automne *du secret*. Paris: Gallimard: 313-324

ANEXOS

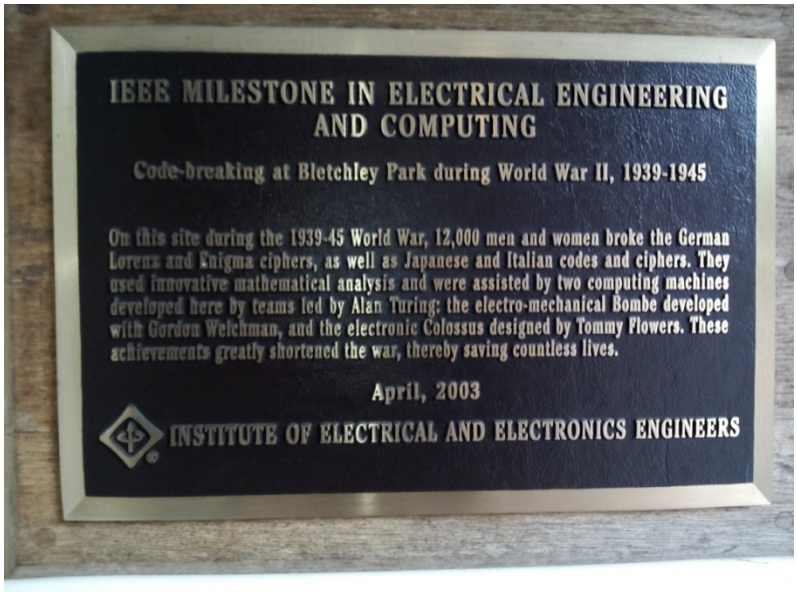


Cartel conmemorativo británico del centeneario del nacimiento de Alan Turing.

Billete de 10 libras inglés conmemorativo el centenario del nacimientos de Turing

Estatua de Turing en Bletchley Park, Inglaterra

Mansión de Bletchley Park, Inglaterra, donde se descifraron los códigos secretos alemanes durante la Segunda Guerra Mundial



Placa conmemorativa de la trascendencia de los descifradores en la Segunda Guerra Mundial. Se hace mención a Turing y a los descifradores no sólo del alemán sino también del italiano y del japonés y a las máquinas Lorenz y Enigma.

Oficina de directivos en Bletchley Park

Escritorios, máquinas y objetos cotidianos en Bletchley Park

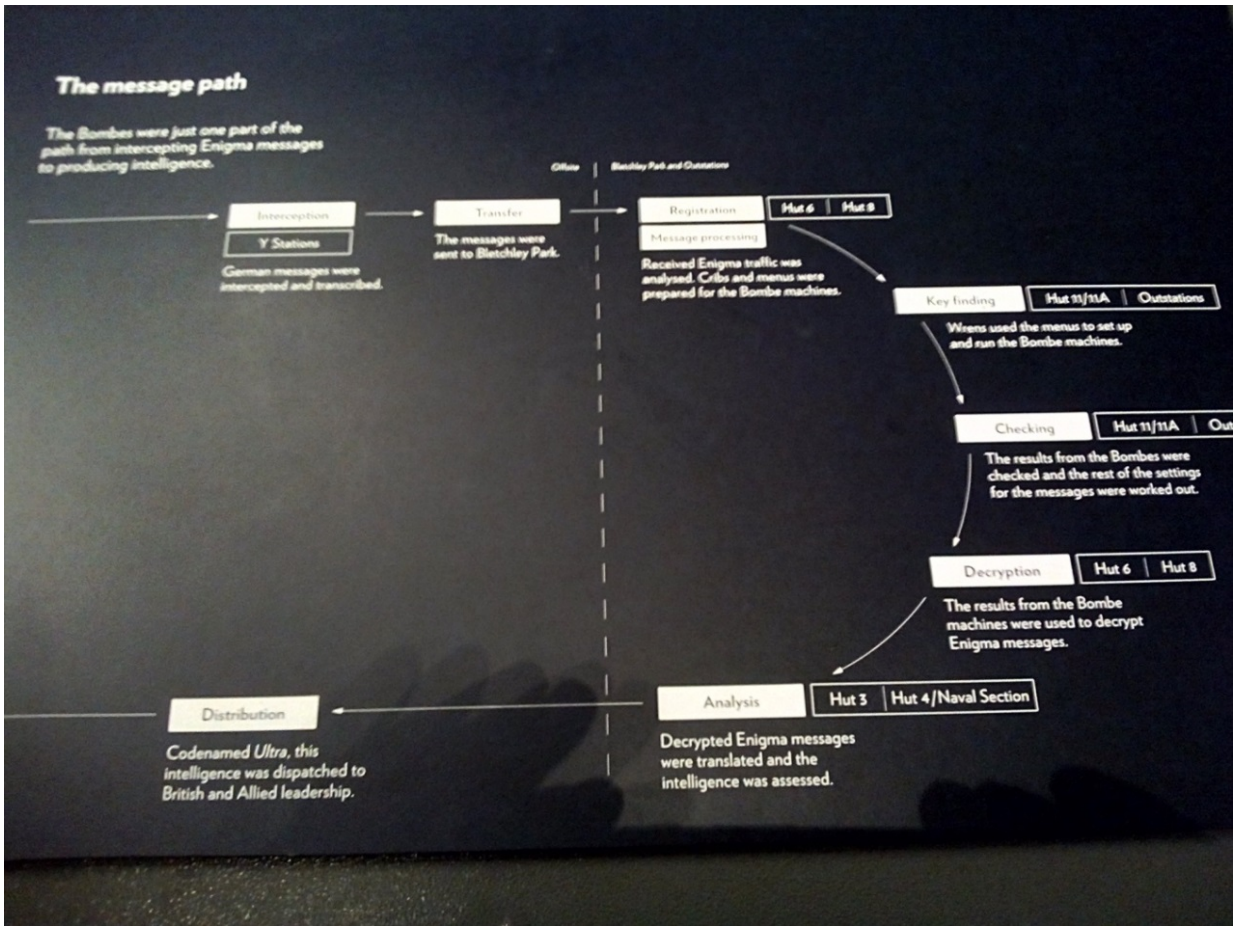
Una d e l as máquinas E nigma en l as q ue trabajaron Turing y s us c olegas en Bletchley Park

Interior de una máquina descifradora británica en Bletchley Park

Una de l as c abañas us adas en el pr oceso de d esciframiento de c ódigos e n Bletchley Park

Ante la Bombe original, máquina creada por Turing y sus colegas para descifrar los códigos de la máquina alemana Enigma.

Rotores originales en Bletchley Park



El paso de los mensajes en Bletchley Park

En la oficina de Alan Turing en Bletchley Park

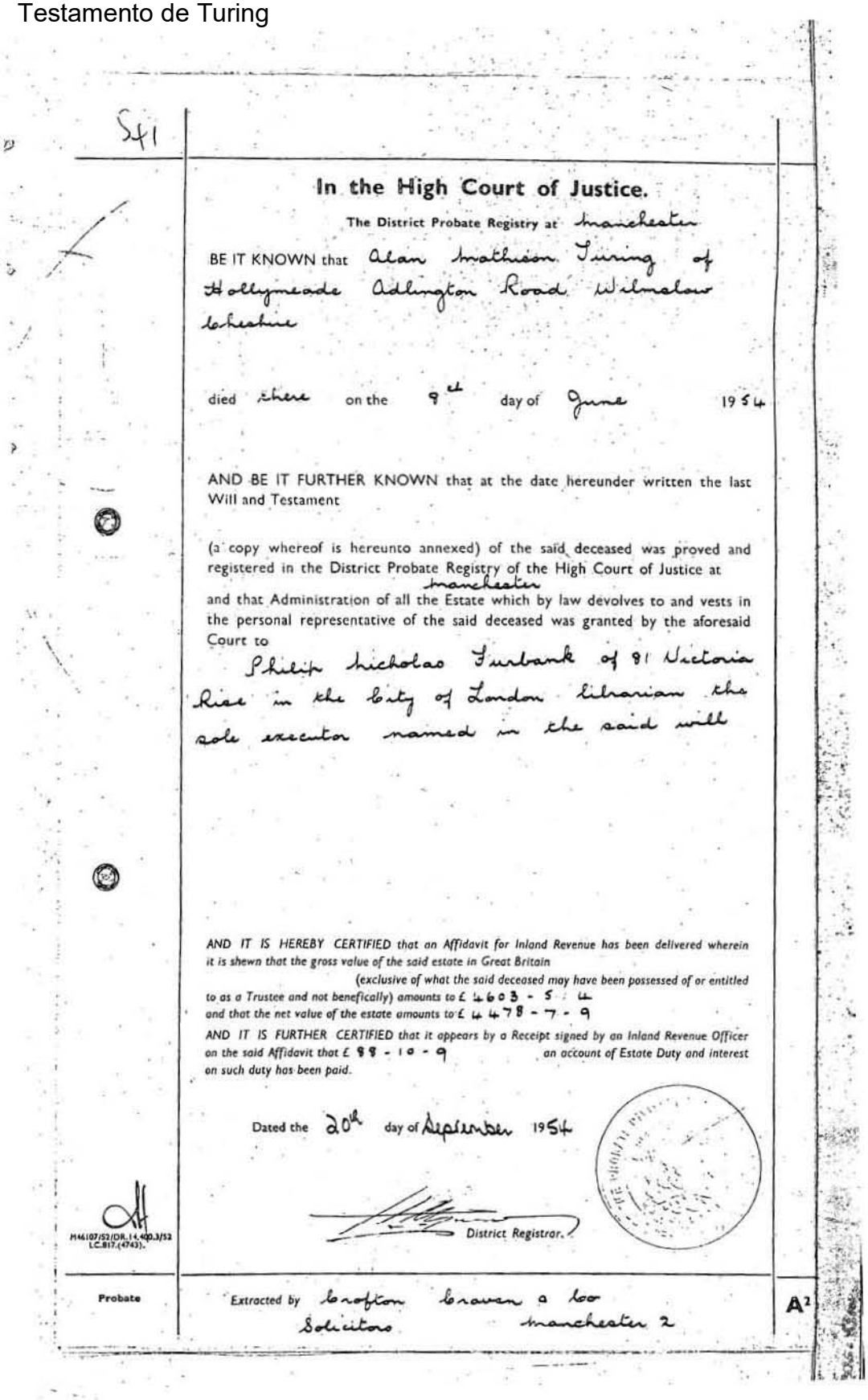
El K ings C ollege de l a U niversidad de Cambridge, d onde fue pr ofesor y se encuentran los archivos y el testamento de Turing

Puerta de entrada a los archivos de Turing en el Kings College de Cambridge

Placa de Turing en el Kings College de la Universidad de Cambridge

Calle cercana al Kings College en Cambridge

Testamento de Turing



541

In the High Court of Justice.

The District Probate Registry at manchester

BE IT KNOWN that Alan Mathison Turing of Hollymeade Addington Road Wilmslow Cheshire

died there on the 9th day of June 1954

AND BE IT FURTHER KNOWN that at the date hereunder written the last Will and Testament

(a copy whereof is hereunto annexed) of the said deceased was proved and registered in the District Probate Registry of the High Court of Justice at manchester and that Administration of all the Estate which by law devolves to and vests in the personal representative of the said deceased was granted by the aforesaid Court to

Philip Nicholas Furbank of 81 Victoria Rise in the City of London Librarian the sole executor named in the said will

AND IT IS HEREBY CERTIFIED that an Affidavit for Inland Revenue has been delivered wherein it is shewn that the gross value of the said estate in Great Britain

(exclusive of what the said deceased may have been possessed of or entitled to as a Trustee and not beneficially) amounts to £ 4603 - 5 - 4

and that the net value of the estate amounts to £ 4478 - 7 - 9

AND IT IS FURTHER CERTIFIED that it appears by a Receipt signed by an Inland Revenue Officer on the said Affidavit that £ 88 - 10 - 9 an account of Estate Duty and interest on such duty has been paid.

Dated the 20th day of September 1954

District Registrar.

M46107/52/DR.14,400.3/52
LC.817.(4743).

Probate

Extracted by Crofton Graven & Co
Solicitors Manchester 2

A2

P.N. Furbank Executor Reginald Smith A Commissioner, etc.

This is the last Will and Testament

of me ALAN MATHISON TURING of Hollymeade Adlington Road Wilmslow University Reader

2. I HEREBY revoke all former Wills and testamentary dispositions made by me

3. I APPOINT Philip Nicholas Furbank of King's College London to be the sole Executor of this my Will Provided that if he shall not survive me then I appoint my brother John Ferrier Turing Solicitor to be the sole Executor hereof

4. I GIVE the following pecuniary and specific legacies namely:-

(a) To the said Philip Nicholas Furbank in case he shall prove this my Will the sum of One hundred pounds

(b) To each of them my said brother John Ferrier Turing and my sister-in-law Joan and nieces Inagh Jean Shuna and Janet all of Glenthorne West Road Guildford who shall survive me the sum of Fifty pounds

(c) To Mrs Clayton of 6 Mount Pleasant Wilmslow in case she shall survive me the sum of Thirty pounds together with an additional sum of Ten pounds for each completed year in which she shall be in my employ from and after the thirtyfirst day of December One thousand nine hundred and fifty three

(d) To Robin Oliver Gandy of University College Leicester University Lecturer all my mathematical books articles and manuscripts but not including any Royalties or other sums of money due to me in respect of any writing of mine

5. I GIVE DEVISE AND BEQUEATH all my estate both real and personal whatsoever and wheresoever not hereby or by any Codicil hereto otherwise disposed of including real and personal estate over which I may have a general power of appointment or disposition Unto such of them my mother Ethel Sarah Turing the said Philip Nicholas Furbank the said Robin Oliver Gandy David Gawen Champernowne of Nuffield College Oxford University Professor and Stanley Neville Johnson of 2 Derby Road Caversham Electrical Engineer as shall be living at the death of my death and if more than one in equal shares

/

6. ANY Executor or Trustee—being a Solicitor or other person engaged in any profession or business shall be entitled to charge and be paid for all acts done by him or his firm in connection with the trusts hereof including acts which a trustee not being engaged in any profession or business as aforesaid could have done personally

IN WITNESS whereof I have to this my Will set my hand this Eleventh day of February —— One thousand nine hundred and fifty four

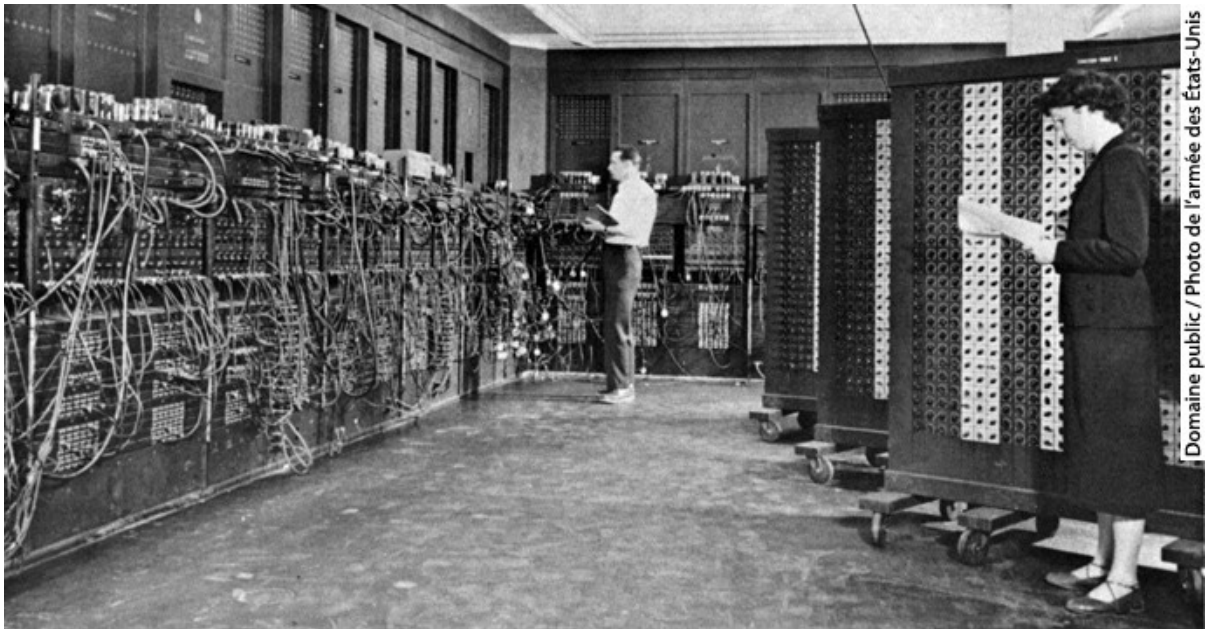
SIGNED by the said Alan Mathison Turing as and for his last Will and Testament in the presence of us who at his request in his presence in the presence of each other all being present at the same time have hereunto subscribed our names as witnesses.

A. M. Turing

Clerks with Letts Greenall,
Solicitors
Manchester, 2.

F. D. Smythe

2



ENIAC (Electronic N umerical I ntegrator and C omputer), construida en 19 46 en Estados U nidos. Se dijo por m ucho t iempo q ue f ue l a primera c omputadora electrónica di gital programable. La bo mba de T uring y ot ras construidas e n Manchester y otros sitios del Reino Unido fueron antes; una de ellas, abajo.