# Los Delitos Informáticos: Experiencia Investigativa en CENDITEL

## Perspectivas de abordajes teóricos

**Endira J. Mora R., Yoselin C. Sánchez A., Oscar E. González D., Daniel A. Quintero R.**

Centro Nacional de Desarrollo e Investigación en Tecnologías Libres – CENDITEL
Mérida, Venezuela
emora@cenditel.gob.ve, ysanchez@cenditel.gob.ve, ogonzalez@cenditel.gob.ve,
dquintero@cenditel.gob.ve

Fecha de recepción: 30/10/2017
Fecha de aceptación: 16/11/2017
Pág: 92 – 106

**Resumen**

Los estudios sobre los Delitos Informáticos se constituyen en un desafío por el carácter multidimensional de la problemática, tomando en cuenta que confluyen en el espacio cibernético individualidades y organizaciones que persiguen objetivos variopintos. Uno de los retos lo configura el abordaje investigativo de tan novedosos fenómenos, presentándose dos líneas teóricas (Críticas-Actividades Rutinarias) que han sido abordadas en CENDITEL por el grupo de "Estudios Estratégicos en Seguridad de la Información", que fueron valoradas por su profundidad argumentativa, la fortaleza para efectuar análisis sistémicos, y la capacidad de canalizar los relacionamientos que se presentan en el ámbito digital.

**Palabras clave**: Delitos Informáticos, espacio cibernético, teoría, crítica, actividades rutinarias.

Como ha argumentado Vold, el crimen es "un comportamiento político y el criminal se convierte de hecho en miembro de un 'grupo minoritario' sin suficiente apoyo público para oponerse al control del poder policial del estado". Aquellos cuyos intereses entren en conflicto con los representados en la ley deben cambiar su comportamiento o, posiblemente, se encontrarán definidos como criminales.

**Richard Quinney**[1]

[1]Texto en su idioma original: As Vold has argued, crime is "political behavior and the criminal becomes in fact a member of a 'minority group' without sufficient public support to dominate the control of the police power of the state." Those whose interests conflict with the ones represented in the law must either change their behavior or possibly find it defined as criminal. (Quinney, R., 1975, p.66)[23]

## Introducción

El Internet ha traído consigo avances poderosos para la humanidad, pero también nuevas complicaciones de orden social, económico y jurídico, ya que para muchos es un espacio fértil de oportunidad delictiva extrapolada de la realidad física al mundo virtual. Esto unido al escaso conocimiento o poco interés por parte de los usuarios, instituciones y gobiernos en medidas de protección ha ocasionado la expansión del espectro de vulnerabilidad. La transformación de la identidad de las personas de una percepción individual hacia una virtualidad colectiva, caracterizada por una vida pública y visible para todos mediante redes sociales a hecho realidad la máxima: "Estoy en red, luego existo" (Malvido, A., 2004, p. 105).[15]

La masificación de los implementos tecnológicos y los beneficios que trae consigo abstraen a los usuarios de los peligros latentes para su integridad personal, tomando en cuenta que "A pesar de las mejoras tecnológicas y de las intensas investigaciones realizadas, el grado en que la tecnología de la información se utiliza para fines ilegales se mantiene estable o tal vez esté incluso aumentando" (ONU, 2010)[22].Este escenario ha empujado a los Estados a tomar medidas encaminadas a la inclusión en sus legislaciones de los delitos informáticos (cibercrimen), concepto que permite englobar la actividad criminal en el espacio de la comunicación abierta y universal en "el ciberespacio"(Felsun Marcus en Miro, F, 2012)[7] y recoge no sólo aquellos comportamientos que hasta hoy se han tipificado como delictivos sino que incluye los que puedan surgir de los avances de las TIC, dando paso a la comprensión de los crímenes cibernéticos no sólo desde las normas sustantivas/adjetivas, sino que permite hacer una interpretación del ilícito para dar respuestas certeras a las víctimas de éste tipo de hechos, porque no basta con plantear un conjunto de medidas reactivas de control, es indispensable saber cómo se interactúa con el ciberespacio, el tipo de relaciones que se establecen en él, qué acciones de protección y prevención son las conducentes. Al cibercrimen pueden vincularse un extenso grupo de actividades delictivas o no, siendo el discernimiento de esas circunstancias lo que permitirá comprender la materia, refiriendo la Organización de Estados Americanos (OEA) al respecto lo siguiente:

> El auge de las tecnologías del último siglo ha traído consigo innumerables avances para la humanidad, pero también otra serie de retos para las autoridades, legisladores e investigadores en las Américas, quienes han tenido que centrarse cada vez más en la persecución y sanción de los delitos cibernéticos, como la pornografía infantil, robo de identidad, acoso cibernético o "hacking". Según estimaciones de LACNIC, el organismo que maneja el Registro de Direcciones de Internet para América Latina y Caribe, el cibercrimen le cuesta a nuestra región alrededor de 90.000 millones de dólares al año (OEA, 2016)[21].

En América Latina son exiguos los estudios sobre la ciberdelincuencia y su incidencia en las víctimas, limitándose a las revisiones de normas sustantivas que permitan castigar el delito cibernético, en los que escasamente se menciona al sujeto pasivo, lo que se explica en parte a la alta cifra negra de la cibercriminalidad, tal como lo esbozan Temperini, Borghello & Macedo: "La cifra negra existente, es consecuencia de la falta de estadísticas oficiales en la

materia, representando un aspecto sustancialmente problemático que impide desarrollar un trabajo serio de observación, análisis y elaboración de estrategias o planes a mediano o largo plazo orientados a combatir el cibercrimen" (Temperini, M., Borghello, C., Macedo, M., 2014, p.2).[26] Por ello, se puede estar produciendo una falsa percepción en relación a los delitos informáticos, originando una afectación en la toma de medidas estratégicas y técnicas dentro de un Estado o gobierno, la propia OEA advierte sobre esta tendencia que es lugar común en el continente:

> Y muchas empresas privadas y otras entidades no gubernamentales siguen mostrándose reacias a reportar ataques o violaciones. Contabilizar el número de incidentes que afectan a los ciudadanos individuales plantea un desafío incluso mayor, en vista del porcentaje incluso más alto de ellos que pasan desapercibidos y no se reportan. Por último, la falta de colaboración generalizada y persistente entre las partes interesadas en todos los niveles dificulta todavía más recoger información sobre violaciones de datos. Las consecuencias netas de todos estos factores son una conciencia menos que adecuada del problema y la continua vulnerabilidad de redes y sistemas de información críticos. (OEA, 2013, p.6)[19].

En el caso de Venezuela, con una población estimada en 30.206.307 habitantes (INE, 2014, p.3)[12] el contexto tecnológico muestra según el "Informe de Cifras del Sector Telecomunicaciones del Primer Trimestre del año 2017" emitido por la Comisión Nacional de Telecomunicaciones (CONATEL) que existen 28.451.182 suscriptores de telefonía móvil, de los cuales 13.517.785 tienen teléfonos considerados Inteligentes. Sobre los datos del uso de la internet para el primer trimestre de 2017 llegó a la cifra de 17.178.743 usuarios con una penetración del 62 %, lo que representaba un incremento de 2,69 % en relación al trimestre anterior (CONATEL, 2017, pp. 7,8,16,18)[5]. Esta realidad nacional viene acompañada de un aumento en la frecuencia de una variedad de incidentes cibernéticos, es relevante destacar que en la última década se ha producido un crecimiento sostenido de los mismos, precisamente en el informe "Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos" se refleja:

> Los actos de vandalismo contra sitios web aumentaron alrededor de 50 %, por ejemplo, mientras que los ataques por Denegación Distribuida de Servicios (DdoS) se incrementaron en 40 %. Uno de los incidentes más importantes se originó en el vandalismo de los portales web de varias instituciones estatales por parte de grupos de hacktivistas nacionales e internacionales. Las autoridades lograron identificar con éxito a los autores mediante el análisis de los registros del historial de los servidores involucrados (OEA, 2014, p. 86)[20].

Estos datos se refieren a información sobre entes públicos y privados, llama la atención la inexistencia de datos vinculados a los particulares, hecho que es reiterativo en documentos emanados de instituciones gubernamentales, incluso la encuesta de "Victimización y Percepción de Seguridad Ciudadana" (INE, 2010)[11] aplicada por el Instituto Nacional de Estadística (INE) no contiene información concisa sobre victimización por delitos Informáticos, pudiendo

deducirse dos cosas: que se obviaron o se aglomeraron junto a datos correspondientes a delitos comunes. No obstante, ninguno de los dos supuestos se justificaría ya que en Venezuela existe un marco normativo que regula el ámbito informático integrado por: la Constitución de la República Bolivariana de Venezuela (1999),[2] la Ley Especial contra los Delitos Informáticos, 2001(LECDI), el Decreto con fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (2001), la Ley de Interoperabilidad (2012) y la Ley de Infogobierno (2013), en las que se establecen los bienes jurídicos protegidos, los deberes y los derechos informáticos, detallándose en la LECDI: los Delitos contra los sistemas que usan tecnologías de Información, la Propiedad, la privacidad de las personas y las comunicaciones, entre otros.

Por tanto, con el propósito de brindar información sobre la victimización individual en Venezuela se hace necesario que instituciones con alcance nacional como el INE efectúen investigaciones tomando para ello el análisis multivariante[3] de la encuesta para ser aplicadas a una muestra significativa de la sociedad venezolana que permita evaluar en un marco cuantitativo los delitos cibernéticos sufridos. En consonancia a lo anterior, tomando como modelo la experiencia del grupo de "Estudios Estratégicos en Seguridad de la Información" de CENDITEL se precisa puntualizar el tipo de actividades llevadas a cabo por las personas en Internet, para dilucidar la percepción de la privacidad, la seguridad y el anonimato, en búsqueda de visualizar los factores de riesgo involucrados, entre otros datos que sirvan para determinar características de ésta clase de fenómenos, proponiendo para ello una edificación pluriteórica que se sustente en las corrientes críticas que efectúan estudios de carácter sistémicos de los problemas delictivos en el marco de los procesos sociales y la Teoría de las Actividades Cotidianas que racionaliza la concomitancia del acto antijurídico como opción y el elemento factorial de la oportunidad. Esta armonización de las corrientes teóricas puede ayudar a focalizar desde una perspectiva social el hecho criminal virtual.

## Premisas Teóricas

La necesidad de un sistema de análisis para los estudios en Seguridad de la información llevó a un profundo debate entre los estudiosos cenditelitas en el área que consideraron que la Teoría Crítica y sus ramificaciones jurídicas/criminológicas contribuirían a mostrar de forma más clara el horizonte investigativo que se pretendía asumir, no sólo por la importancia que se le da al factor social, sino que además valora elementos trascendentes como la lucha de clases y las relaciones de dominación, lo que se ajusta a los conflictos actuales que se emanan de la realidad virtual.[4]

[2]Donde se estable el derecho/garantía de Habeas Data.

[3]El Análisis Multivariante es un conjunto de métodos estadísticos y matemáticos, destinados a describir e interpretar los datos que provienen de la observación de varias variables estadísticas, estudiadas conjuntamente(Cuadras, C., 2014, p.11)[6]

[4]**Nota aclaratoria de los autores**: En el presente artículo se hace referencia a dos corrientes teóricas que han tenido un importante desarrollo en el grupo de "Estudios Estratégicos en Seguridad de la Información". Empero, no se han asumido de forma excluyente y constantemente se esta abierto a revisar y enriquecer los estudios con otras visiones científicas.

Las teorías del conflicto como semillero de la llamada criminología crítica concentra su interés en el control social, estudiando la conducta delictiva dentro del marco de la lucha de clases, de la confrontación entre sectores y grupos sociales. Tomando referencialmente estos enunciados se puede manifestar que el ciberespacio constituye un lugar donde confluyen los intereses de clase y se reproducen las pugnas del mundo físico. En un plano mucho más preciso, la criminología crítica se ha mostrado como un continuador dentro de las corrientes *neomarxistas* de las teorías del conflicto, acentuando el examen de la lucha de clases y la dominación de los poderosos, intentado romper con los paradigmas de la criminología tradicional, presentando una perspectiva macrosocial y política, que se hace pertinente para evaluar al ciberespacio con una profundidad que la escuela tradicional obvia. Buscando los pilares fundacionales de ésta corriente del pensamiento, debemos remontarnos al siglo XIX donde el italiano Enrico Ferri se erige como uno de los iniciadores de los estudios criminales sobre una base social, expresando en varias de sus apreciaciones que no era la pobreza en sí, sino la distribución desigual de la riqueza la que determina el nivel de la delincuencia, pero además coloca al delincuente como sujeto que es afectado por las realidades de la sociedad:

> Tuvimos ya varias ocasiones de hacer notar que una de las diferencias fundamentales entre la escuela clásica y la positiva del derecho criminal, consiste en que mientras aquella estudia el delito en sí, como ente jurídico abstracto, la positiva lo considera como el hecho de un hombre, como causa y efecto de la constitución orgánica y psíquica del delincuente, unida a las influencias del ambiente físico y social. Es decir, que mientras en la escuela clásica el delincuente esta en segunda linea, aun cuando se hayan estudiado las causas modificativas de su imputabilidad moral, en la escuela positiva, por el contrario, el delincuente esta siempre en primera linea (Ferri, E, 1982, p. 163)[8]

Evidentemente éste replanteamiento estuvo marcado por la influencia de las corrientes filosóficas que habían irrumpido en los estudios sociales de la época, siendo justamente Karl Marx quien atinó a postular teóricamente la lucha de clases como motorizadora de la historia, en su epístola a Pavel Vasilievich Annenkov, acota:

> ¿Qué es la sociedad, cualquiera que sea su forma? El producto de la acción recíproca de los hombres. ¿Pueden los hombres elegir libremente esta o aquella forma social? Nada de eso. A un determinado nivel de desarrollo de las facultades productivas de los hombres, corresponde una determinada forma de comercio y de consumo. A determinadas fases de desarrollo de la producción, del comercio, del consumo, corresponden determinadas formas de constitución social, una determinada organización de la familia, de los estamentos o de las clases; en una palabra, una determinada sociedad civil. A una determinada sociedad civil, corresponde un determinado orden político (état politique), que no es más que la expresión oficial de la sociedad civil (Marx, K., 1846, pp. 1-2).[16]

Es exponencialmente relevante el planteamiento del filosofo treviriano, ya que sin dedicar su disertación específicamente a la criminalidad su aporte encaja perfectamente en el análisis

del acto antijurídico, al colocar la constitución de la sociedad civil como derivada de las fases productivas o de consumo, deja en claro que existen elementos que imponen las formas de relacionamiento humano bajo un esquema de dominación (Burguesía/Proletariado). Habría que referir partiendo de Marx que en una sociedad se producen conductas consideradas como ilegales por los actores dominantes pero ésta definición de criminalidad pasa a ser una herramienta del statu quo para someter a las fuerzas que se muestren antagónicas al poder constituido. El debate creció en prolijidad el siglo XX, destacando William Joseph Chambliss que era incisivo en que la pugna de clases es la energía que sustenta el sistema capitalista, indicando:

> Capitalist societies, where the means of production are in private hands and where there inevitably develops a division between the class that rules (the owners of the means of production) and the class that is ruled (those who work for the ruling class),creates substantial amounts of crime, often of the most violent sort, as a result of the contradictions that are inherent in the structure of social relations that emanate from the capitalist system (Chambliss, W., 1975, p. 150)[3][5]

Estas contradicciones que nos expone el criminólogo estadounidense son certeras y nos muestra que desde las corrientes críticas se puede hacer ese estudio sistémico que nos puede conducir a los elementos propios de la criminalidad con rasgos tecnológicos de la sociedad actual. Por su parte, Richard Quinney quien colocó como uno de sus preceptos inamovibles a la *"Justicia Social"* reflexionaba con tono crítico en relación al crimen, sosteniendo una postura coincidente con Chambliss, orientando:

> The powerful interests are reflected not only in the definitions of crime and the kinds of penal sanctions attached to them, but also in the legal policies on handling those defined as criminals. Procedural rules are created for enforcing and administering the criminal law. Policies are also established on programs for treating and punishing the criminally defined and programs for controlling and preventing crime. From the initial definitions of crime to the subsequent procedures, correctional and penal programs, and policies for controlling and preventing crime, those who have the power regulate the behavior of those without power (Quinney, R., 1975, p.66)[23][6].

[5]Las sociedades capitalistas, donde los medios de producción están en manos privadas y donde inevitablemente se desarrolla una división entre la clase que gobierna (los propietarios de los medios de producción) y la clase que es gobernada (los que trabajan para la clase dominante), crea cantidades sustanciales de crimen, a menudo del tipo más violento, como resultado de las contradicciones que son inherentes a las estructura de las relaciones sociales que emanan del sistema capitalista.**(Traducción de los autores del artículo)**

[6]Los intereses de los poderosos se reflejan no solo en las definiciones de crimen y los tipos de sanciones penales que se les atribuyen, sino también en las políticas legales sobre el manejo de aquellos que son definidos como criminales. Las normas procedimentales se crean para hacer cumplir y administrar la ley penal. Las políticas también se establecen en los planes para el tratamiento y sanción de los programas y figuras penales para el control y la prevención del delito. Desde las definiciones iniciales del delito hasta los procedimientos posteriores, los planes correccionales y penales, y las políticas para controlar y prevenir el delito, quienes tienen el poder regulan el comportamiento de aquellos que no lo tienen. **(Traducción de los autores del artículo)**

Los intereses de los poderosos y su influencia en la realidad del siglo XXI no ha cambiado, y por el contrario la expansión de las redes informáticas a hecho que la dominación se amplíe y llegue a adoptar mecanismos de control insospechados en años anteriores. En la obra "La nueva criminología" de los británicos Ian Taylor, Paul Walton y Jock Young se puntualiza sobre la necesidad de ahondar en los estudios de la criminalidad para crear nuevos esquemas que comprendan la heterogeneidad de variables involucradas y que no sean controladas por los factores dominantes, subrayando:

> Para nosotros, como para Marx y para otros nuevos criminólogos, la desviación es normal, en el sentido de que en la actualidad los hombres se esfuerzan conscientemente (en las cárceles que son las sociedades contemporáneas y en las cárceles propiamente dichas) por afirmar su diversidad humana. Lo imperioso es, no simplemente «penetrar» en esos problemas, no simplemente poner en tela de juicio los estereotipos ni actuar como portadores de «realidades fenomenológicas alternativas». Lo imperioso es crear una sociedad en la que la realidad de la diversidad humana, sea personal, orgánica o social, no esté sometida al poder de criminalizar (Taylor, I., Waltony, P., Young, J., 1997, p. 298).[25]

El reto se muestra dificultoso ya que las visiones hegemónicas construyen las realidades conforme a sus intereses y no sólo los sujetos, grupos o comunidades son objetivos de la criminalización, sino que ahora incluso grupos étnicos, religiosos o naciones enteras son marcadas y excluidas al ser concebidas como potencialmente amenazantes para los detentadores del poder. En síntesis la ruta para revertir esa unipolaridad criminalizadora que de manera omnipotente decide qué es una conducta desviada y qué lo normalmente aceptable pasa porque la sociedad en conjunto asuma el protagonismo de evaluar cuáles son verdaderamente las causas que llevan a cometer un delito, no para transcribirlo como letra muerta de un código sino para palpar dinámicamente el hecho social, en ese misma línea reflexiona Antonio García-Pablos de Molina:

> Dado que cada sociedad tiene el crimen que merece, una política seria y honesta de prevención debe comenzar con un sincero esfuerzo de autocrítica, revisando los valores que la sociedad oficialmente proclama y practica. Pues determinados comportamientos criminales, a menudo, entroncan con ciertos valores (oficiales o subterráneos) de la sociedad cuya ambivalencia y esencial equivocidad ampara "lecturas" y "realizaciones" delictiva (García, A., 2012, p. 97)[9]

El investigador ibérico nos pone a reflexionar sobre el contexto cibernético que abarca todas las aristas de nuestra existencia y generan un conjunto de interrogantes: ¿Los modos de relacionamiento de la sociedad actual son consecuencia del modelo tecnológico?, ¿El cibercrimen es una desviación natural de quienes buscan la diversidad humana en el ciberespacio?, ¿Puede contribuir la tecnología a emanciparnos de los intereses de los poderosos?, ¿Los cibercrímenes son una categoría delictual creada por las élites capitalistas para mantener la desigualdad de clases en el ciberespacio?. Ese conjunto de cuestiones pueden ser reflexionadas bajo las premisas

de las corrientes críticas que dan la posibilidad de estudiar el conjunto social sin desconocer la indiviudalidad, pero sobre todo conscientes de la lucha de clases que muchas veces de manera solapada se da, pero que en definitiva es la que moldea las realidades.

Teniendo éste portentoso sistema analítico para realizar el examen de la totalidad social, sin embargo se nos hace preciso acompañar el mismo con un complemento académico que contribuya a sustentar las propuestas de estudio, que conforme a nuestra experiencia grupal la "Teoría de las Actividades Cotidianas" trabajada por Lawrence Cohen y Marcus Felson reúne esas condiciones. Los mencionados autores en *"Social Change and Crime Rate Trends: A Routine Activity Approach"* afirman que producto del cambio constante de la sociedad se han dado transformaciones en las actividades que cotidianamente se realizan, como por ejemplo el desplazamientos de un lugar a otro, aumento del tiempo que se pasa fuera de casa, el traslado de propiedades y el movimiento del dinero, donde existen cada vez mayor número de oportunidades para delinquir, puesto que hay más objetos de valor expuesto, sobre todo en los sitios donde las víctimas y los delincuentes tienen mayor contacto y este aumento de la oportunidad delictiva dependerá de la convergencia en espacio y tiempo de tres factores:

> We argue that structural changes in routine activity patterns can influence crime rates by affecting the convergence in space and time of the three minimal elements of direct-contact predatory violations: (1) motivated offenders, (2) suitable targets, and (3) the absence of capable guardians against a violation. We further argue that the lack of any one of these elements is sufficient to prevent the successful completion of a direct-contact predatory crime, t and that the convergence in time and space of suitable targets and the absence of capable guardians may even lead to large increases in crime rates without necessarily requiring any increase in the structural conditions that motivate individuals to engage in crime (Cohen, L., Felson, M., 1979, p. 589).[4][7]

Al respecto señala Charles Tittle en una disertación sobre los "Desarrollos teóricos de la Criminología" en la que desglosa los tres presupuestos exhibidos por Cohen y Felson, que la vinculación temporal/espacial para la concreción de la acción predatoria debe armonizar diversas variables en las que además de los sujetos activos y pasivos deben coincidir motivaciones, objetivos y omisiones, enfatizando el autor norteamericano:

> Una vigilancia débil se produce cuando muchas actividades se llevan a cabo fuera del hogar y cuando las personas están con frecuencia en compañía de extraños. La disponibilidad de

[7]Sostenemos que los cambios estructurales en los patrones de actividad rutinaria pueden influir en las tasas de criminalidad al afectar la convergencia en espacio y tiempo de los tres elementos mínimos de las violaciones predatorias de contacto directo: (1) delincuentes motivados, (2) objetivos adecuados, y (3) ausencia de guardianes capaces de controlar una violación. Además argumentamos que la falta de cualquiera de estos elementos es suficiente para evitar la finalización con éxito de un delito de depredadores por contacto directo, y que la convergencia en el tiempo y el espacio de los objetivos adecuados y la ausencia de guardianes capaces pueden incluso llevar a grandes aumentos en las tasas de criminalidad sin que necesariamente se requiera un aumento en las condiciones estructurales que motivan a las personas a participar en el crimen.**(Traducción de los autores)**

> blancos para la criminalidad predatoria se relaciona con el valor y el tamaño de los objetos que van a ser robados o con lo atractivo de los objetos que van a ser violados o asaltados. El tercer elemento,ofensores motivados, se asume generalmente como una constante en tiempo y espacio. Esto es, lo que los teóricos han asumido más o menos que siempre existen infractores potenciales que –dadas ciertas oportunidades creadas por los blancos disponibles y no custodiados– actuarán (Tittle, C., 2006, p. 26).[27]

No obstante, motivado a la diferencia propia del contexto material al virtual es necesario ajustar las bases teóricas para que puedan ser aplicadas al espacio cibernético. Es de destacar que las máximas propuestas por Cohen y Felson son coincidentes con los delitos informáticos pero con algunos matices: pudiendo reflejarse en lo relativo al tiempo y espacio, que ya no se necesita la interacción directa entre agresor y víctima, pero los infractores potenciales ajustan la realidad para hacer sus blancos disponibles. Asimismo, lo deseable del bien jurídico protegido cambia, no necesariamente priva su valor monetario, sino cuán sensible es el activo de información para la víctima a quien se le sustrajo (Siendo tal vez la inercia el punto más diferenciado entre la materialidad del delito y su variante informática). En cuanto, al papel de la vigilancia, que tradicionalmente es ejercida por las autoridades policiales, queda ahora circunscrito a personal técnico capacitado en áreas como informática forense que se apoya en sistemas de detección para asumir labores tanto preventivas como reactivas (Ejemplo de ello los CERT - Computer Emergency Response Team[8]). Sumando algunos criterios al respecto, el catedrático Fernando Miró Llinares sugiere una responsabilidad más personalizada para la vigilancia en su escrito titulado "La Oportunidad Criminal en el Ciberespacio":

> (...) La víctima va a ser prácticamente la única que puede incorporar guardianes capaces para su autoprotección. Al no existir en éste ámbito criminológico distancias físicas ni guardianes formales institucionalizados, el uso cotidiano que haga de las TIC y en especial la incorporación (o no) de sistemas digitales de autoprotección, serán determinantes a la hora de convertirse en víctima del cibercrimen (Miró, F., 2011, p. 45).[17]

Como hemos podido observar de esta revisión académica las dos propuesta teóricas que han conducido varias de nuestras investigaciones pueden complementarse y ciertamente no representan mutuamente una antítesis. Es necesario entender, que el marco de exploración del mundo cibernético requiere de premisas generales y sustantivas que se engranen para emanar una interpretación homogénea de la problemática.

## Experiencia institucional conforme a las bases teóricas

El Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL), se ha erigido sobre la idea de investigar para que el conocimiento y las tecnología libres potencien los procesos que coadyuven a la independencia y soberanía de la nación, en consonancia

[8]Equipo de Respuesta ante Emergencias Informáticas**(Traducción de los autores)**

con su Acta Constitutiva Estatutaria que resalta: "(...) tiene como objeto impulsar a nivel nacional las tecnologías de información y comunicación con estándares libres, promoviendo la investigación y el desarrollo de productos innovadores que conduzcan a la soberanía tecnológica del país" (CENDITEL, 2008).[2] El contexto nacional reseñado en la parte introductoria del artículo evidenció un escenario en donde los temas de seguridad y defensa informática, han sido abordados de manera aislada desde los planos estratégico y técnico, lo que ha llevado a una visión sesgada de la problemática, que no tiene una apreciación integral sobre el riesgo informático, repercutiendo en la expansión de las vulnerabilidades ante los factores externos.

Frente a esta realidad se asumió en CENDITEL con empeño desde el año 2014 la tarea de consolidar un equipo multidisciplinario compuesto por abogados, criminólogos y politólogos entre otros profesionales que se encargaran de hacer estudios sobre una temática que requería tratamiento dentro del Estado venezolano, decidiéndose crear un grupo de "Estudios Estratégicos en Seguridad de la Información" que encajara en los parámetros de la Ley de Infogobierno, concretamente en el Título V "De los subsistemas que conforman el Sistema Nacional de Protección y Seguridad Informática" (Ley de Infogobierno, 2013)[14] y que estuviera en la capacidad de iniciar una línea de investigación con una propuesta teórica definida, que además brindara asesoría especializada a instituciones estatales, junto con la tarea de formar a talento humano emergente en consonancia a los cuatro procesos que motorizan nuestra institución contenidos en la cuarta cláusula estatutaria: "Gestión del conocimiento y apropiación de la tecnología libre; Reflexión y fundamentación de la tecnología libre; Investigación en tecnología libre; y Desarrollo de tecnología libre". (CENDITEL, 2008)[2]

Dentro de la variedad de propuestas teóricas que se barajaron para fundamentar los procesos investigativos, se buscó la concomitancia con los principios cenditelitas y se encontró que la Teoría Crítica presentaba elementos coincidentes especialmente en su variante de estudios tecnológicos. Precisamente en un estudio realizado por Quintero, D., (2016)[24] como parte de su investigación en CENDITEL titulado "Las Investigaciones de fenómenos tecnológicos a la luz de la Teoría Crítica", en uno de sus extractos, que se acompaña de las ideas de Theodor Adorno (Adorno, Theodor, 1998)[1]), se expresa:

> Dentro de las ciencias sociales los planteamientos teóricos basados en los llamados estudios críticos pueden ser una corriente orientadora en las propuestas investigativas que relacionan lo social y tecnológico. Al respecto, en una profunda reflexión sobre el cambio social experimentado por la creciente ramificación de la tecnología en la cotidianidad humana, expresaba Adorno (1998): "Un mundo como el actual, en el que la técnica ocupa una posición central, produce hombres tecnológicos, acordes con la técnica" (p. 88). Esta disertación desentraña una preocupante tendencia en las sociedades del siglo XXI, y es la estructuración de sistemas políticos opresivos dirigidos por los "hombres tecnológicos" (pp. 139-140).

Esa interacción socio/tecnológica de la Teoría Crítica llevó a penetrar en su rama jurídico/criminológica, efectuándose en nuestro centro el estudio denominado "Aportes Criminológicos a las Políticas Públicas de Ciberseguridad y Ciberdefensa como Problemas

Legales, Técnicos y Sociales en Venezuela", que desde el estudio de González, O., (2016)[10] profundizó en las realidades tecnológicas nacionales y regionales que se manejan bajo un esquema de dominación por parte de las potencias tecnológicas mundiales en detrimento de las naciones en vías de desarrollo, reseñando:

> De esta manera, se realizó una exploración de la relación entre la Criminología y el Ciberespacio desde las diversas corrientes teóricas criminológicas: positivistas, de la Escuela Clásica, estructuralistas, funcionalistas y de la Criminología Crítica, siendo esta última la más apropiada para utilizarla como teoría central para establecer las implicaciones y producir aportes criminológicos al desarrollo de las políticas de Ciberseguridad y Ciberdefensa como fenómenos legales, técnicos y sociales. (s/p)

Desde la perspectiva complementaria manejada en el grupo de "Estudios Estratégicos en Seguridad de la Información" la "Teoría de las Actividades Cotidianas" realizó la asesoría del estudio "La victimización por delitos informáticos en el contexto de las Tecnologías de la Información y la Comunicación: Análisis en una muestra de estudiantes universitarios" (Oduber, J.,2015)[18], que constituye una de las pocas experiencias en materia de victimización por delitos violatarios de la privacidad que se ha realizado en Venezuela, con potencial para ser usado como modelo para un proceso de validación estadística a escala nacional sobre delitos informáticos. Aportando conclusiones sobre el rol de la cibervíctima por el tipo de información que sobre sí y su quehacer cotidiano hace pública o visible en la web, siendo ésta la que se pone en riesgo latente debido a las acciones que lleva a cabo en internet.

## Reflexiones finales

El grupo de "Estudios Estratégicos en Seguridad de la Información" ha mostrado ser una experiencia novedosa que a pesar de su novel existencia se ha ido potenciado por el interés de sus investigadores que han entendido la importancia manifiesta de la Seguridad de la Información para el Estado venezolano, proponiendo ante el conjunto de desafíos que se presentan propuestas investigativos con rigor teórico y fortaleza académica. Las corrientes críticas sobre los cuales se han apoyado nuestros estudios nos han permitido desmontar las estructuras ideológicas de sectores dominantes para visibilizar las grandes desigualdades que se proyectan desde el mundo cinético al virtual. Infiriendo que la valoración de los delitos informáticos sin un adecuado contraste teórico nos puede llevar a una simple tipificación que sea complaciente con los parámetros hegemónicos quedando de lado la comprensión social del delincuente informático, sus motivaciones y el entorno social en el que se desenvuelve. Sí la visión crítica nos ha brindado la oportunidad de una percepción "macrosocial, la "Teoría de las Actividades Cotidianas" ha asomado un abanico de posibilidades para estructurar la evaluación dirigida a a entender lo "microsocial" del ciberdelincuente, ese quehacer que se zambulle en la mente del infractor para percibir el carácter motivacional de la acción del "cracker"[9]

[9]Cracker es el término que define a programadores maliciosos y ciberpiratas que actúan con el objetivo de violar ilegal o inmoralmente sistemas cibernéticos, siendo un término creado en 1985 por hackers en defensa del

## Esquema de relacionamiento teórico

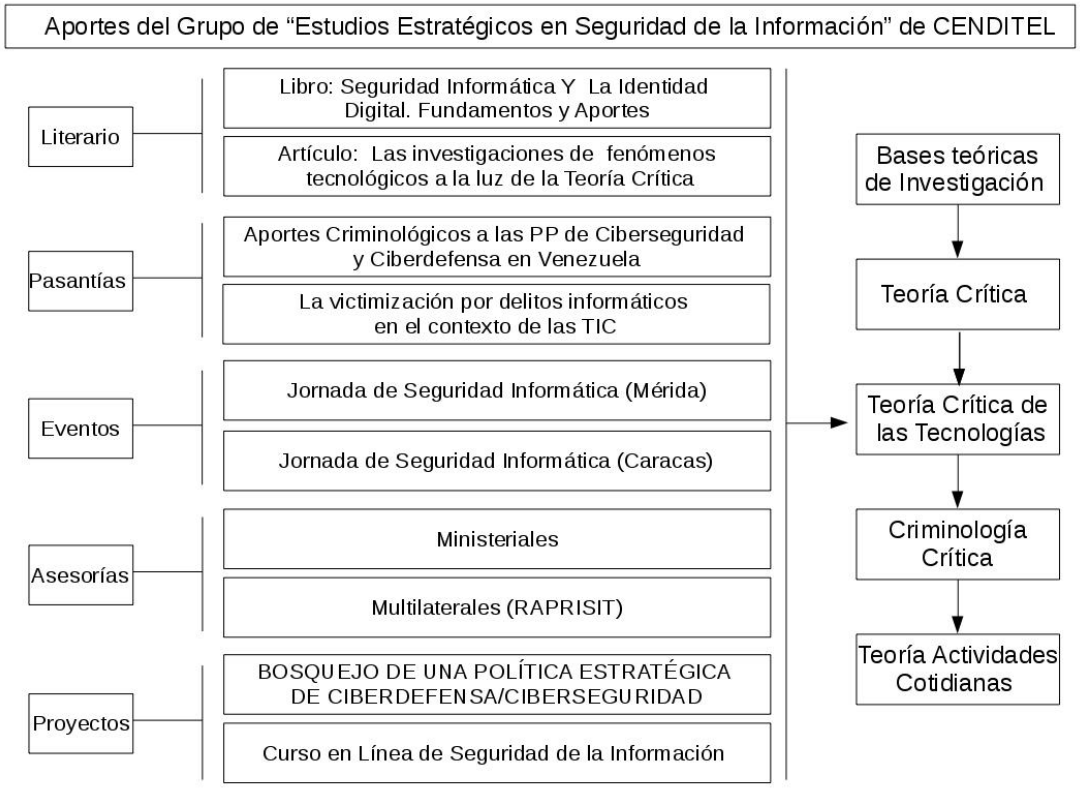


Figura 1: Relacionamiento teórico

## Bibliografía

[1] Adorno, T. (1998): *Educación para la emancipación*. Colección: Pedagogía: Raíces de la memoria. Traducción de Jacobo Muñoz. En Quintero, D. (2016). Las Investigaciones de fenómenos tecnológicos a la luz de la Teoría Crítica. Revista CLIC Nro. 13, Año 7 – 2016. ISSN: 2244-7423.

[2] CENDITEL (2008). *Acta Constitutiva Estatutaria del Centro Nacional de Desarrollo e Investigación en Tecnologías Libres CENDITEL*. Gaceta Oficial Nº 38.906.

[3] Chambliss, W. (1975). *Toward a Political Economy of Crime. Theory and Society*, 2(2). Recuperado de http://www.jstor.org/stable/656788

uso periodístico del término.[13]

[4] Cohen, L., Felson, M. (1979). *Social Change and Crime Rate Trends: A Routine Activity Approach*. American Sociological Review. Recuperado de https://www.scribd.com/document/255237557/Cohen-Felson-Social-Change-and-Crime-Rates-Trends-A-Routine-Activities-Approach

[5] CONATEL (2017). Presentación Cifras I trimestre 2017. Recuperado de http://www.conatel.gob.ve/informe-cifras-del-sector-tercer-trimestre-2016/

[6] Cuadras, C. (2014) *Nuevos métodos de análisis multivariante*. CMC Editions. Recuperado de http://www.ub.edu/stat/personal/cuadras/metodos.pdf

[7] Felson, M. en Miro, F. (2012). *Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons. Madrid-España.

[8] Ferri, E. (1892). *Estudios de Antropología Criminal*. Tercera edición: La España Moderna, Madrid. Recuperado de http://fama2.us.es/fde/ocr/2005/estudiosDeAntropologiaCriminal.pdf

[9] García, A. (2012). *La prevención del delito en un estado social y democrático de derecho*. Universidad Complutense de Madrid. Recuperado de http://www.cienciaspenales.net/files/2016/11/3_LA-PREVENCION-DEL-DELITO.pdf

[10] González, O. (2016). *Aportes Criminológicos a las Políticas Públicas de Ciberseguridad y Ciberdefensa como Problemas Legales, Técnicos y Sociales en Venezuela*. Universidad de Los Andes. Facultad de Ciencias Jurídicas, Políticas y Criminológicas, Escuela de Criminología. Unidad Académica de Formación Integral y Pre-Profesional.

[11] INE (2010). Encuesta Nacional de Victimización y Percepción de Seguridad Ciudadana 2009 (ENVPSC- 2009) Documento Técnico. Recuperado de https://www.oas.org/dsp/pdfs/encuestavictimizacion2009.pdf

[12] INE (2014). Venezuela Entorno Social y Económico Recuperado de http://www.tss.gob.ve/wp-content/uploads/2014/08/II-Perfil-Venezuela-1-de-abril-2014.pdf p.3

[13] Informática Hoy (2017). *Qué es un Cracker?* Recuperado de https://www.informatica-hoy.com.ar/aprender-informatica/Que-es-un-Cracker.php

[14] Ley de Infogobierno (2013). Gaceta Oficial, 40.274, octubre 17, 2013.

[15] Malvido, A. (2004). *Cibercultura: estoy en red, luego existo. Los retos culturales de México*, 2004. Recuperado de http://biblioteca.diputados.gob.mx/janium/bv/ce/scpd/LIX/ret_cul_mex.pdf#page=96

[16] Marx, K. (1846). *Carta a Pavel Vasilievich Annenkov*. Universidad Complutense de Madrid. Recuperado de http://webs.ucm.es/info/bas/es/marx-eng/cartas/oe1/mrxoe117.htm

[17] Miró, F. (2011). *La Oportunidad Criminal en el Ciberespacio. Revista Electrónica de Ciencia Penal y Criminología*. Artículos ISSN 1695-0194RECPC 13-07 (2011). Recuperado de http://criminet.ugr.es/recpc/13/recpc13-07.pdf

[18] Oduber, J. (2015). *La victimización por delitos informáticos en el contexto de las Tecnologías de la Información y la Comunicación: Análisis en una muestra de estudiantes universitarios*. Universidad de Los Andes. Facultad de Ciencias Jurídicas, Políticas y Criminológicas, Escuela de Criminología. Unidad Académica de Formación Integral y Pre-Profesional.

[19] OEA (2013). Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos. Recuperado de https://www.sites.oas.org/cyber/Documents/2013%20-%20Tendencias%20en%20la%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe%20y%20Respuestas%20de%20los%20Gobiernos.pdf p.6

[20] OEA (2014). Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos. Recuperado de https://www.sites.oas.org/cyber/Documents/2013%20-%20Tendencias%20en%20la%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe%20y%20Respuestas%20de%20los%20Gobiernos.pdf p.86

[21] OEA (2016). Ciberdelito: 90.000 millones de razones para perseguirlo. Recuperado de http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-063/16

[22] ONU (2010). 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Recuperado de https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf p.2.

[23] Quinney, R. (1975). *Conflict Theory of Crime*. From Richard Quinney, Criminology (Boston: Little, Brown, 1975), pp. 37–41. Recuperado de http://fasnafan.tripod.com/conflicttheoryofcrime.pdf

[24] Quintero, D. (2016). *Las Investigaciones de fenómenos tecnológicos a la luz de la Teoría Crítica*. Revista CLIC Nro. 13, Año 7 – 2016. ISSN: 2244-7423.

[25] Taylor,I., Waltony, P. & Young, J. (1997). *La nueva criminología. Contribución a una teoría social de la conducta desviada*. Arnorrortu editores, Buenos Aires. Recuperado de http://escuelasuperior.com.ar/instituto/wp-content/uploads/2017/05/ian-taylor-paul-walton-jock-young-la-nueva-criminologia.pdf

[26] Temperini, M., Borghello, C., Macedo, M. (2014). *La cifra negra de los delitos informáticos: Proyecto ODILA*. Recuperado de ODILA https://www.ekoparty.org/archivo/2014/eko10-La_cifra_negra_de_los_delitos_informaticos.pdf

[27] Tittle, C. (2006). *Los desarrollos teóricos de la criminología.* Justicia Penal Siglo XXI. Una Selección de Criminal Justice 2000. Edición de Rosemary Barberet & Jesús Barquín. Recuperado de https://www.ncjrs.gov/pdffiles1/nij/213798_spanish/213798_spanish.pdf