

Coloquio Preparatorio
24 – 27 Septiembre 2013, Antalya (Turquía)
Sección III: Sociedad de la información y Derecho penal

COLOMBIA*

Johannes F. Nijboer

(A) Objeto del cuestionario (ver Anexos 1 2)

Las preguntas de esta Sección tratan generalmente del “Ciberdelito”. Este término se entiende en el sentido de dar cobertura a las conductas criminales que afectan a intereses asociados con el uso de la tecnología de la información y comunicación (TIC), como el funcionamiento adecuado de los sistemas de ordenadores y de internet, la intimidad y la integridad de los datos almacenados o transferidos a o a través de las TIC o la identidad virtual de los usuarios de internet. El denominador común y rasgo característico de todas las figuras de ciberdelitos y de la investigación sobre ciberdelitos puede hallarse en su relación con sistemas, redes y datos de ordenadores, de un lado, y con los sistemas, redes y datos cibernéticos, del otro. El ciberdelito cubre delitos que tienen que ver con los ordenadores en sentido tradicional y también con la nube del ciberespacio y las bases datos cibernéticas.

Si se precisa cualquier aclaración, por favor, contactar con el Relator General, Prof. Dr. Johannes F. Nijboer por email: J.F.Nijboer@law.leidenuniv.nl

(B) Cuestiones Generales

(1) ¿Existen definiciones (jurídicas o socio-jurídicas) para la aplicación de las TI y de las TIC en el contexto del procedimiento penal (incluida la práctica forense)? ¿Cómo están reflejadas estas definiciones conceptuales en la doctrina científica, la legislación, las decisiones judiciales, y las prácticas pertinentes en el contexto del proceso penal?

R.

Por tecnologías de la información existe un pacífico común acuerdo que se trata de un concepto desarrollado gracias a la aparición en el mundo de la disciplina ‘INFORMÁTICA’. Misma que trata sobre el procesamiento automatizado de información, proceso que se surte sobre tres funciones básicas que han de desarrollar los sistemas, casi que por sí mismos, de ahí justamente es que proviene el termino, ya que la información es por primera vez en el mundo de ser almacenada, tratada o transmitida casi que por sí misma.

Por Tecnologías de la Información y las Comunicaciones, ha de comprenderse que se trata de la capacidad de comunicar, de transmitir*, esa información que se trata, almacena y transmite a lo largo del mundo.

Si bien es muy cierto que las formas, los vehículos de los que se valen las TIC, para transmitir, comunicar la información que se procesa son en ocasiones distintos debido al uso del espectro electromagnético, tan solo los medios desarrollados hasta el momento cumplen la mera función de comunicar, de transmitir, pero al evaluar su contenido o los efectos que ésta información transmitida ha de cumplir en el mundo real una vez sea procesada por un sistema automatizado de información van a ser los mismos, por eso es necesario remitirse a la base, al nacimiento de aquella información para ver que desde un punto abstracto, de ‘lege ferenda’ no han de concebirse como fenómenos aislados el uno del otro, así las cosas, se procede a contestar el interrogante formulado en precedencia.

Si, “En otras ramas del Derecho ajenas al Derecho Penal, se conciben definiciones de la prueba documental, en la misma ley 527 de 1999 que le brinda fuerza probatoria al mensaje de datos, en las cuales encontramos que al definir o intentar regular la evidencia digital se remite de forma expresa a la legislación procesal civil para el manejo de esos medios probatorios que, legalmente, se equiparan a la prueba documental.”¹

Un análisis sistemático para contestar en debida forma este interrogante, compele a observar como desde el C. P. P., Colombiano, Ley 906 de 2004, ARTÍCULO 275. ELEMENTOS MATERIALES PROBATORIOS Y EVIDENCIA

* Atención: El texto que se publica constituye la última versión original del informe nacional enviado por el autor, sin revisión editorial por parte de la Revista.

¹ *Ibíd.* p. 149.

FÍSICA. "Para efectos de este código se entiende por elementos materiales probatorios y evidencia física, los siguientes:

g) El mensaje de datos, como el intercambio electrónico de datos, internet, correo electrónico, telegrama, télex, telefax o similar, regulados por la Ley 527 de 1999 o las normas que la sustituyan, adicionen o reformen"

En la norma acabada de citar, se hace una remisión expresa de la legislación procesal penal la LEY 527 DE 1999. Dicha norma cuenta con su respectivo artículo definitorio respecto de elementos básicos para el funcionamiento de las denominadas 'TIC'.

En la práctica forense en Colombia existen documentos, resoluciones que circulan al interior de la Fiscalía General de la Nación, donde sin apartarse del contenido de la ley 527, se trata el tema de la cadena de custodia y se siguen principios básicos del estatuto o desarrollos norteamericanos en tanto al primer respondiente y todo el manejo de la escena del crimen.

Los desarrollos logrados por la Ciencia, la Doctrina en este ámbito, han sido recogidos por la doctrina a punto de exigir para la garantizar mediante presunta autenticidad que, si los primeros respondientes han de seguir el procedimiento de cadena de custodia expreso en los documentos restringidos a los funcionarios de la policía judicial y/o partes del respectivo proceso, tales elementos probatorios gozaran de dicha presunción de autenticidad.

- (2) ¿Existen instituciones específicas y / o grupos de trabajo involucrados en la aplicación de las TIC en el sistema penal?

En Colombia existen varios grupos o entidades encargadas de velar por ello, desde el CISPA, cuyas siglas refieren: "La Comisión Intersectorial de Seguimiento al Sistema Penal Acusatorio-CISPA- fue creada mediante el Decreto 261 de enero 28 de 2010 , modificado por el Decreto 491 de 2012 del Ministerio de Justicia.", hasta en los organismos de policía judicial como el Cuerpo Técnico de Investigación Judicial (CTI), existen organismos como el "Grupo de Delitos Informáticos del Cuerpo Técnico de Investigación", encargados de tales labores.

(3) ¿Existen organizaciones (empresas) privadas (comerciales) que ofrecen servicios relacionados con las TIC en el sistema penal? Si es así, ¿puede dar ejemplos? ¿Qué límites tienen que ser observados?

En repetidas ocasiones el país se contratan servicios por agencias del gobierno a organicémonos o empresas privadas (comerciales), expertas en el asunto como: "ADALID ABOGADOS".

(C) Información e inteligencia: construyendo posiciones de información¹ (information positions) para aplicación de la ley

(1) ¿Qué técnicas relacionadas con las TIC se utilizan para la construcción de posiciones de información por las agencias de aplicación de la ley?

Entiéndase por posición de la información, la construcción de segmentos de información segura, es decir, ofrecer determinada 'seguridad' sobre la autenticidad de información que reposa en medios digitales, así, la Fiscalía General de la Nación en varias de las resoluciones de circulación restringida, se hace alusión a los medios de carácter informático que han de tomarse para la salvaguardan de información que se desee brindar de la presunción de autenticidad.

Presunción que en 'principio' se garantiza mediante estampas cronológicas de seguridad, es decir, a la información en medios digitales se le agrega una estampa que permite saber la fecha de recibo de la información en los correspondientes laboratorios de la Fiscalía General de la Nación, mediante 'sellos' o estampas de 'seguridad' denominados SHA-1, SHA-256 y el poco usado Md-5.

(2) ¿A qué tipo de bases de datos públicas (por ejemplo, bases de datos de ADN) y privadas (por ejemplo, el Registro de Nombre de Pasajero o los datos financieros como los datos de SWIFT) tienen acceso las agencias de la aplicación de la ley?

A cualquiera que se encuentre en el territorio nacional mediante orden de la autoridad competente, que para el caso del sistema penal acusatorio adoptado por Colombia, la autoridad ha de ser el juez de control de garantías.

(3) ¿Pueden aplicarse las técnicas consideradas como minería de datos y comparación de datos? Si es así, ¿pueden utilizarse estas técnicas para crear perfiles de posibles autores o grupos de riesgo? Si es así, ¿se han desarrollado herramientas especiales para las agencias de aplicación de la ley?

Los procesos de minería de datos y comparación de los mismos, son procedimientos que realiza la policía judicial en sus labores de indagación o investigación.

De cosecha propia, en nuestra nación no existen desarrollos que se puedan ofrecer, el software hasta hora en uso de tales entidades se corresponde con los ofrecidos por empresas Vgr, Mattica.

Su uso, dado la relación de los mismos con una posible afectación de derechos fundamentales está bajo previa autorización del juez de control de garantías quien como se deduce de todas las menciones realizadas en precedencia, se trata de un juez que vela por la protección de los derecho fundamentales de las partes del proceso.

(4) ¿Pueden utilizarse medidas coercitivas (por ejemplo, la interceptación de las telecomunicaciones) para la construcción de posiciones de información?

En desarrollo de labores de investigación o indagación que realiza la policía judicial a órdenes del Fiscal, no existen limitaciones para el ejercicio de tales medidas de interceptación de comunicaciones, previa autorización del juez de control de garantías.

(5) ¿Qué actores privados (por ejemplo, proveedores de internet o empresas de telecomunicaciones) conservan o están obligados a conservar información para las agencias de aplicación de la ley?

Todos las que en la prestación de su servicio involucren información que, por autorización del juez competente sea requerida.

(6) ¿Qué actores privados pueden proporcionar o están obligados a proporcionar información a las agencias de aplicación de la ley?

Todos las que en la prestación de su servicio involucren información que, por autorización del juez competente sea requerida.

(7) ¿Existe control judicial de la construcción de posiciones de información?

Como ya se dijo, la autorización del juez de control de garantías es básico elemento para el desarrollo de tales labores cuando impliquen afectación de los derechos fundamentales de un sujeto involucrado en el proceso.

(D) Las TIC en la investigación penal

(1) ¿Pueden las agencias de aplicación de la ley llevar a cabo intervenciones en tiempo real a) de datos sobre el tráfico , b) sobre el contenido de los datos?

Prevía autorización del juez de control de garantías, tales facultades le son propias a los investigadores de la situación en el caso en concreto.

1 La construcción de las posiciones de información es parte de la denominada actuación policial basada en la inteligencia. Se puede definir la actuación policial basada en la inteligencia como un marco conceptual de llevar a cabo la actividad policial como un proceso de organización de la información que se permite a las agencias de aplicación de la ley en sus tareas preventivas y represivas.

Coloquio Preparatorio Sección III

2

(2) ¿Pueden las agencias de aplicación de la ley tener acceso / congelar / investigar / secuestrar los sistemas de información sobre: a) datos sobre el tráfico.

En el Estado de Derecho de la República de Colombia si, sólo que la redacción que se formula en la pregunta, propiamente el significado de los verbos: -Congelar/ Investigar / Secuestrar /, denota que desde su misma formulación se desconocen aspectos técnicos de la informática y por tanto ofrecer una respuesta a una pregunta así formulada no colabora con el cabal entendimiento del objeto del estudio, -EL DELITO INFORMÁTICO.

-Captar- datos informáticos que conforman los datos de tráfico habilita el desarrollo de las tres actividades por las que se pregunta. Y se insiste, en Colombia tales actividades se pueden desarrollar siempre que se cuente con la previa autorización del juez de control de garantías.

b) el contenido de los datos?

Una vez captada la información con la respectiva autorización judicial, sobre el contenido de los mismos, al todavía no existir completo entendimiento por las autoridades de ni el legislador, no se ha notado que tales datos se tratan del bien jurídico de "representación por excelencia".²

(3) ¿Se puede obligar a las empresas de telecomunicaciones o proveedores de servicios a compartir los datos con las agencias de aplicación de la ley?

En Colombia es posible solicitar a tales empresas la información requerida por autoridad judicial a quien habrá que demostrar la pertinencia, proporcionalidad y necesidad de tales elementos al proceso. Plena claridad en el asunto ofrece la Sentencia T – 216 de 2004, Magistrado Ponente Eduardo Montealegre Lynett, al desarrollar el tema en el siguiente aparte: "La información privada, será aquella que por versar sobre información personal o no, y que por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio."

En caso de incumplimiento, ¿hay medidas coercitivas o sanciones?

La obstaculización de la administración de justicia en Colombia es sancionada

² Ibídem. P. 60.

4) ¿Pueden las agencias de aplicación de la ley realizar videovigilancia?

La expectativa razonable de intimidad puede verse afectada por tales medidas, según el caso en concreto habría que revisarlo, claro que en lugares públicos, en presencia de las señales que así lo indiquen no veo inconveniente en ello. Ya para afectar la intimidad de las personas, tal procedimiento ha de seguirse previa autorización del juez constitucional.

¿Pueden obligar a las personas físicas o jurídicas a cooperar?

La colaboración con la administración de justicia es un deber ciudadano, salvo claro, los claros límites del 'nemo tenetur se ipso accusare'. Esto es, el derecho a la no autoincriminación. En casos como el que se pregunta, nuevamente exige valorar el caso en concreto y acorde al mismo se ha de solicitar a la autoridad competente la orden, so pena, de la respectiva sanción.

(5) ¿Pueden o deben aplicar las agencias de aplicación de la ley grabación audiovisual de los interrogatorios (sospechosos, testigos)?

La estructura del proceso penal acusatorio vigente en nuestra república, así lo exige. Pero en determinados casos no será necesaria la medida.

(E) Las TIC y la prueba (La cadena de etapas: recogida / almacenamiento / retención / producción / presentación / valoración de la prueba electrónica)

(1) ¿Existen reglas sobre la prueba específicas para la información relacionada con las TIC?

Ya se hizo referencia al tema al tratar sobre la remisión expresa que realiza el C.P.P., colombiano a la Ley 527 de 1999, que le brinda fuerza probatoria y eleva el mensaje de datos al rango de prueba documental y exige de la misma determinadas condiciones ya descritas en precedencia.

(2) ¿Existen reglas sobre la integridad (por ejemplo, manipulación o procesamiento incorrecto) y seguridad (por ejemplo, hacking) de la prueba relativa a las TIC?

Tal como la legislación nacional comprende al tipo de evidencias por las que se inquiriere en este aparte, a favor de garantizar el principio de mismidad, 'mismidad' o la integridad del material probatorio, se le aplicaran a estas los sellos o estampas cronológicas y se ha de diligenciar un incipiente formato de cadena de custodia que ya se maneja en nuestra latitud.

Propiamente hablando, a nivel de la informática se maneja unos formatos 'Sha-1 y Sha-256' entre otros desarrollos que intentan brindar de 'integridad' y 'seguridad' tales evidencias.

(3) ¿Existen reglas sobre la admisibilidad (incluido el principio de legalidad procesal) de las pruebas que son específicas de la información relacionada con las TIC?

En general, apenas para cubrir de una mera presunción de autenticidad se exigen ciertos requisitos conforme a las guías que usa el FBI. Tales se encuentran descritas en 'the guide for the first responder'.

En el mismo se recatan otros aportes, por ejemplo: IOCE (Internacional Organization Of Computer Evidence) y Standard and Principles Scientific Working Group on Digital Evidence (SWEDGE), para el manejo de evidencias digitales.

Pero en general, cualquier mecanismo está abierto a las partes y lo exigible en vigencia de la actual legislación procesal penal colombiana, es que no se violen los derechos humanos, es decir, que las medias por lo menos estén acordes a ellos.

(4) ¿Existen reglas específicas sobre el descubrimiento y revelación de la prueba relacionada con las TIC?

Entre las ya manifestadas en tanto la Cadena de Custodia, tal aporte ha de seguir las ritualidades descritas en la ley procesal penal colombiana en tanto la respectiva la audiencia y que a las partes se les garantice, entre otras, la contradicción de las mismas.

(5) ¿Existen reglas especiales para la valoración (valor probatorio) de la prueba relacionada con las TIC?

Reglas especiales para estos efectos NO. Al valor probatorio de la evidencia en estos ámbitos se le aplican criterios generales para valorar todo el material probatorio en general.

(F) Las TIC en la etapa de juicio

(1) Cómo puede o debe introducirse en el juicio la prueba relacionada con las TIC?

En la respectiva audiencia de acusación o preparatoria, o que según el caso y en el orden mencionado, la fiscalía ha de presentar las pruebas que pretenderá llevar a vista judicial.

En atención al C. P. P., artículo 382, se debe comprender que una 'prueba' se puede introducir a juicio sin importar su esencia o naturaleza, siempre que no se viole el ordenamiento jurídico, mismo que al elevar a rango de prueba documental un mensaje de datos que es definido en la misma ley cómo "La información generada, enviada, recibida,

almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax”.

Luego, la ley postula al mensaje de datos con la misma fuerza probatoria que una prueba documental, en tal sentido, se exige entonces una remisión al Código de Procedimiento Civil para evaluar las características básicas de la ‘prueba’ documental.

Así las cosas, el material probatorio relativo a evidencia digital, según lo dispuesto en nuestra Constitución Política, C.P.P. Ley 906 de 2004, Código de Procedimiento Civil, Ley 527 de 1999 y normas concordantes, la prueba relacionada con las (TIC), se introduce siguiendo los mismos parámetros de una prueba documental.

(2) ¿Pueden realizarse interrogatorios a distancia (por ejemplo, conexiones vía satélite)?

De la lectura del C.P.P., Ley 906 de 2004, artículo 386, se infiere que la respuesta a este interrogante es afirmativa: “IMPEDIMENTO DEL TESTIGO PARA CONCURRIR. Si el testigo estuviere físicamente impedido para concurrir a la audiencia pública donde se practicará la prueba, de no hallarse disponible el sistema de audio vídeo u otro sistema de reproducción a distancia, ésta se realizará en el lugar en que se encuentre, pero siempre en presencia del juez y de las partes que harán el interrogatorio.”

(3) ¿Pueden utilizarse técnicas digitales y virtuales para la reconstrucción de los hechos (asesinatos, accidentes de tráfico)?

Claro, asistido por expertos cualquier medio que no viole el ordenamiento jurídico es permitido.

(4) ¿Pueden utilizarse técnicas audiovisuales para presentar pruebas en el juicio (en su forma más simple: imágenes y sonido)?

Si, no veo limitación para ello, repito, siempre que no se viole el ordenamiento.

(5) ¿Pueden sustituirse los expedientes penales en "papel" por otros electrónicos? ¿Se ha avanzado hacia la digitalización de los documentos del juicio?

En la Central de Servicios Judiciales se entregan actualmente copias de las audiencias en disco compacto (Cd) o disco de video digital (Dvd), procedimiento que se realiza al público en general dada la característica de algunas públicas en curso del proceso. En éstas ha de constar toda la discusión y sustentación que del devenir procesal se haya presentado en la respectiva audiencia. Existen audiencias reservadas donde la posibilidad de acceso a ellas es ‘restringido’ para algunas partes del proceso, por su misma naturaleza entonces, han de permanecer bajo el velo de audiencias reservadas.

Coloquio Preparatorio Sección III

3

Anexo 1

John A.E. Vervaele

1. Definición de la Sociedad de la Información? Elementos esenciales de una definición No existe un concepto único de sociedad de la información que predomine. La doctrina se esfuerza en la concreción de las definiciones y valores del concepto y se centran en cuestiones económicas, técnicas, sociológicas y culturales. La sociedad post moderna a menudo es caracterizada como una "sociedad de la información", debido a la amplia disponibilidad y uso de la Tecnología de la Información y la Comunicación (TIC). La definición más común de la sociedad de la información pone el énfasis en la innovación tecnológica. El procesamiento, almacenamiento y transmisión de la información han dado lugar a la aplicación de las tecnologías de la información y la comunicación (TIC), y a las relacionadas con la biotecnología y la nanotecnología, en casi todos los rincones de la sociedad. La sociedad de la información es una sociedad postindustrial en la que la información y el conocimiento son los recursos clave y están jugando un papel fundamental (Bell, 1973 y 1979).

Sin embargo, la sociedad de la información no solamente se define por la infraestructura tecnológica, sino más bien como un fenómeno multidimensional. Bates (1984) señaló que cualquier sociedad de la información es una red compleja, no sólo de infraestructura tecnológica, sino también una estructura económica, un patrón de relaciones sociales, modelos de organización y otras facetas de la organización social. Por lo tanto, es importante no centrarse sólo en el aspecto tecnológico, sino también en los atributos sociales de la sociedad de la información, incluido el impacto social de la revolución de la información en las organizaciones sociales, comprendido el sistema de justicia penal.

Por otra parte, la era postmoderna de la tecnología de la información transforma el contenido, la accesibilidad y la utilización de la información y el conocimiento en las organizaciones sociales, incluido el sistema de justicia penal. La relación entre el conocimiento y el orden ha cambiado radicalmente. La transformación de las comunicaciones en tecnología instantánea de información ha cambiado la manera en

la que la sociedad valora el conocimiento. En esta era de rápidos cambios, la estructura de la autoridad tradicional se está debilitando y está siendo sustituida por un método alternativo de control social. La aparición de un nuevo paradigma tecnológico basado en las TIC se ha traducido en una sociedad en red (network society) (Castells1996), en la que las principales estructuras y actividades sociales se organizan en torno a las redes de información procesada electrónicamente. Existe una transformación aún más profunda de las instituciones políticas en la sociedad en red: el surgimiento de una nueva forma de Estado (Estado en red) que gradualmente sustituye a los Estados-nación de la era industrial. En esta era de rápidos cambios, la estructura de la autoridad tradicional se está debilitando y está siendo sustituida por un método alternativo de control social (sociedad de la vigilancia). La transición del Estado-nación al Estado en red es un proceso organizativo y político impulsado por la transformación de la gestión, representación y dominación política en las condiciones de la sociedad en red. Todas estas transformaciones exigen la difusión de redes interactivas múltiples como la forma de organización del sector público.

La información y el conocimiento son recursos clave de la sociedad de la información, que afectan a la estructura social y política de la sociedad y al Estado y que afectan a la función, estructura y contenido del sistema de justicia penal.

2. La interrelación de los cuestionarios de las cuatro secciones En primer lugar, deberíamos utilizar una definición de trabajo común. Está claro que la referencia a los delitos informáticos es demasiado restrictiva para nuestro tema y que la expresión "derecho penal de la información o delitos relacionados con la sociedad de la información" tampoco tiene un significado claramente fijado.

Por estas razones, tenemos que usar una definición común y un enfoque limitado.

En cuanto a la definición, propongo utilizar el concepto de ciberdelito, pero con una definición que incluye una amplia variedad de nuevos fenómenos y desarrollos.

El denominador común y rasgo característico de todas las figuras de ciberdelitos y de la investigación sobre ciberdelitos puede hallarse en su relación con sistemas, redes y datos de ordenadores, de un lado, y con los sistemas, redes y datos cibernéticos, del otro. El ciberdelito cubre delitos que tienen que ver con los ordenadores en sentido tradicional y también con la nueva del ciberespacio y las bases datos cibernéticas.

Coloquio Preparatorio Sección III

4

En segundo lugar, ya que esta es un área muy amplia, debemos centrarnos en los ámbitos más interesantes en los que nuestras resoluciones puedan aportar valor añadido. El resultado de los debates con los cuatro relatores generales es que nos centremos en los siguientes bienes jurídicos en el ámbito del ciberdelito:

1. La integridad y funcionalidad del sistema de las ciber-TIC (delitos CID) 2. Protección de la privacidad 3. Protección de la personalidad digital 4. Protección frente a los contenidos ilícitos 5. Protección de la propiedad (incluidos los derechos de propiedad intelectual) 6. Protección contra los actos cometidos exclusivamente en el mundo virtual 7. Protección del sistema de cumplimiento de las normas (delitos de incumplimiento [non-compliance offences])

3. Bibliografía

Daniel Bell, *The Coming of Post-Industrial Society*, New York, Basic Books , 1976.

Manuel Castells, *The Rise of the Network Society. The Information Age: Economy, Society and Culture Volume 1*. Malden: Blackwell. 2d Edition, 2000

S. Sassen, *The global city* , New York-London, Princeton University Press, 2d edition, 2001.

U.Sieber, *Mastering Complexity in the Global Cyberspace*, in M. Delmas-Marty & M Pieth. *Les chemins de l'harmonisation Pénale*, Paris 2008, 127-202.

APORTE MICHAEL MEEK NEIRA.

Profesor John A.E. Vervaele,

Sobre lo que usted menciona es completamente cierto afirmar lo siguiente.

Es verdad que estamos en una sociedad de la información, cada vez el mundo gira en torno a ella, pero que hace posible tal condición? Como unificar o llevar al derecho penal vigente en nuestros pueblos a hacer un efectivo frente a estas nuevas manifestaciones criminales?

Lo primero es comprender en que consiste, en la obra que se encuentra a su disposición: Delito Informático y Cadena de Custodia lo digo todo. Allí, al hablar de la triada informática realizo un análisis transversal de lo que debe entenderse como actos propios del 'cibercriminal'.

Parto de un análisis elemental y culmino por señalar que sucede al interior de los sistemas automatizados de información, computadores, sistemas informáticos u ordenadores, para permitir al hombre la ejecución de comandos que reflejen el dolo del autor o memorias de sus acciones.

Basta de expandir el derecho penal para hacer descripciones casuistas que muchas veces no sean fáciles de encuadrar al caso concreto, debemos terminar con baches en las descripciones típicas que permitan la impunidad del 'cibercriminal'.

Luego de una lectura atenta de la obra, espero sea de fácil comprensión, es posible ver al ser humano en la sociedad de la información, en necesidad de compartir información y datos para llevarlos a ejecutar comandos, desarrollar distintas actividades o representar audio, imágenes o video.

El bien jurídico de 'lege ferenda' "De la protección de la información y los datos" informáticos, es un interés del que se vale la sociedad de la información, tal como usted y yo en este momento, para representar cualquier contenido o de tener la posibilidad de acceder a su ordenador, de verificar si dispone de impresora conectada y hasta hacer impresiones de documentos, con lo que sin dudarlo, estaría modificando el mundo, siendo lo propio permitirnos llevar nuestra mente tan lejos como la realidad lo permita.

En ese orden de ideas, es posible controlar y dirigir desde un ordenador artefactos o dispositivos electro – mecánicos, realizando la voluntad de algunos científicos fuera de la misma órbita terrestre, en marte, donde el común denominador a ellos radica en el procesamiento de información automatizada al interior de sus procesadores informáticos que pueden representarse las ordenes a seguir, gracias al bien tutelado en el ordenamiento colombiano.