



# RETOS JURÍDICOS PARA EL ETHOS HUMANO EN LAS PLATAFORMAS DIGITALES DE INTERNET

Leonardo José Pereira Meléndez  
leopermelcarora@gmail.com  
Universidad Nacional de la Seguridad,  
UNES-Lara  
Pontificia Universidad Católica Santa Rosa,  
Caracas.  
<https://orcid.org/0000-0002-3720-319X>

Fecha de recepción: 20 /01/2022  
Fecha de aprobación: 17/12/2022

## RESUMEN

El contexto dialéctico y altamente dinámico de la sociedad del presente siglo XXI, reta a explorar y concretar alternativas en todos los sectores, y en particular el informático como sendero hacia una conspicua convivencia humana, signada por los nóveles valores que son mediados a través de los sistemas jurídicos. Una de las vertientes distorsionantes para la sociedad global la representa el delito informático, por tanto, el objeto central del presente ensayo lo constituyó la acción de identificar los retos

jurídicos para el ethos humano en las plataformas digitales de internet. Se trastocaron las formas comportamentales humanas que han edificado un imaginario sociocultural complejo en la materia. Fue aplicado un muestreo documental, que facilitó la selección efectiva en los planos conceptuales, jurídicos y contextuales de los textos que sirvieron de base para los análisis e interpretaciones correspondientes. Los hallazgos son el resultado de una causa ardua de información contrastada, con el fin de avalar su legitimidad. La conclusión más relevante a destacar es el reto de unificación de la norma en diversos niveles geopolíticos, teniendo como punto de inicio la formulación unificada de tipificaciones del delito de este tipo en cada país y posteriormente en las regiones continentales.

**Palabras clave:** Retos jurídicos, gnoseología del delito informático, teleología del delito informático, riesgos informáticos.



## Legal challenges for the human ethos in digital internet platforms

### ABSTRACT

The dialectical and highly dynamic context of the society of the present XXI century, challenges us to explore and specify alternatives in all sectors, and in particular the computer science as a path towards a conspicuous human coexistence, marked by the new values that are mediated through the legal systems. One of the distorting aspects for global society is represented by computer crime, therefore, the central object of this essay was to describe the legal challenges for the human ethos in digital internet platforms. It is about disrupting the human behavioral forms that have built a complex sociocultural imaginary. A documentary sampling was developed, which facilitated the effective selection in the conceptual, legal and contextual planes of the bibliographic sources used for the corresponding analyzes and interpretations. The findings are the result of an arduous cause of analysis of the information, triangulated and contrasted, in order to guarantee its legitimacy. The most relevant conclusion to highlight is the challenge of unifying the norm at various geopolitical levels, having as a starting point the unified formulation of criminal offenses of this type in each country and later in the continental regions.

**Keywords:** Legal challenges, gnoseology of computer crime, teleology of computer crime, IT risk.

### INTRODUCCIÓN

El siglo XXI trajo consigo una avasallante dinámica de cambios orgánicos que ha modificado la cotidianidad en la convivencia y las relaciones humanas en lo cultural, económico, social, así como en todas las instituciones de la sociedad. En razón de ello, la colectividad global que ha conocido y se ha hecho parte de la concepción digital informática, en la que el uso de redes informáticas y de múltiples aplicaciones coadyuva con las actividades humanas, también se ha apreciado atónita la esfera delictiva que en paralelo ha emergido en las últimas décadas. De esta manera, el ethos informático es altamente variable, reconfigurando tanto la convivencia social colectiva como la conducta individual del ser humano. Esta adquiere sentidos, significados propios y etéreos particulares para el trabajo en redes informáticas que extreman lo impersonal en su uso.

En relación al nuevo ethos social, Delgado (2020) precisa la nueva taxonomía cognitiva del presente siglo mediadas por lo discrecional humana y la tecnología. La sociedad en su aspiración por controlar los



entornos próximos, ha clasificado y designado nombres contextuales, como el de “Generación Z”, esta se refiere a las personas nacidas a finales del siglo XX e inicios del XXI, siendo la peculiaridad primordial de este conjunto humano su habilidad en utilizar y aplicar cotidianamente los acervos tecnológicos digitales, haciéndolos parte de su vida, y no admiten opiniones o representaciones externas a esa realidad.

Frente al ethos que traspasa lo social y lo cognitivo a lo informático global y local, los sistemas jurídicos y sus componentes conceptuales, tipificaciones y procedimientos se han tenido que adaptar a esta realidad. Cabe destacar que fue en los años setenta del siglo XX, cuando se reportaron los primeros delitos de este orden, como corolario de los reportajes periodísticos publicados en la época, teniéndose como reseña histórica la novela *1984* del eximio escritor George Orwell (1903 – 1950), donde uno de los personajes creados por Eric Arthur Blair, vigilaba y fichaba la vida de los habitantes mediante el uso de métodos tecnológicos. De tal forma que la gnoseología sobre el delito informático no se ha detenido, constriñendo a los jurisperitos nuevas concepciones adaptadas a esta realidad, más aún en la medida en que nuevas

aplicaciones van emergiendo de la informática para uso en la internet, y junto a ellas deviene una teleología del delito informático que muta permanentemente y configura nuevos umbrales.

En este orden de ideas, se tiene tanto a las individualidades o colectividades sociales, y económicas impactadas por los riesgos informáticos, sobre cuyo interés radican los estudios y los acaecimientos adaptativos propios de los sistemas de justicia. En Venezuela, al igual que en el resto de países latinoamericanos hasta el resto del mundo, la inseguridad personal ha trascendido las figuras delictivas tradicionales, asumiendo vertiginosamente diversos ámbitos de las actividades digitales, y su disposición como anomalía nacional, no se limita a contornos y fronteras virtuales.

El objetivo fundamental del presente ensayo gira en torno a identificar los retos jurídicos para el ethos humano en las plataformas digitales de internet, para ello se planteó una reflexión e interpretación de cada uno de las múltiples aristas sobre la contigüidad gnoseológica del delito informático y las pléyades jurídicas que se derivan de la informática global, así mismo los enfoques doctrinales jurídicos de la informática como escenario para la identificación de los delitos de este orden. A



ello le fueron adicionadas las estadísticas de los riesgos informáticos (IT) y las razones tipificadas en el orden jurídico. Finalmente pueden apreciarse los retos identificados en el apartado de las conclusiones.

## DESARROLLO

### *Contigüidad gnoseológica del delito informático*

Un acercamiento conceptual hacia la definición universal del delito informático todavía no ha sido aprehendido, motivado entre otras razones, a las disímiles configuraciones de los sistemas jurídicos globales; a la afluencia de argumentaciones económicas y políticas propias de la sociedad globalizada. Por tanto, solo para efectos del presente ensayo, se han estimado cuatro ideas substanciales que de una manera u otra tienden a homogenizar las doctrinas que se tienen sobre el mismo, sin intentar llegar a una presunción conceptual. Así que como *lege ferenda* (la ley por hacer) a nivel global, se ha optado por asumir de plano la conducta humana criminológica que hace meritoria la tipificación en cualquier país de estas contravenciones como delitos informáticos.

Las cuatro ideas referidas tanto a la naturaleza de la norma y los límites mismos

de esta son: 1) el uso de del computador para infligir la norma, 2) los daños a bienes jurídicos informáticos, 3) una acción antijurídica usando la internet, y 4) el delito informático en su significación plural. La primera se asocia a Hernández (2009), el cual reseña que para el año 1978, se identificó públicamente un delito de este tipo, con la irrupción de un daño patrimonial informático, considera que:

...el acento debe ponerse en que los ordenadores pueden ser usados por el autor del delito no sólo como instrumentos para cometer el mismo sino también como objeto del delito. Este autor incluyó entre los *computer crimes* los delitos de sabotaje informático, robo de información digitalizada y programas, espionaje industrial, hurto de tiempo de uso del ordenador, robos de mercancías por manipulación de datos o fraudes financieros. (pág. 231).

La segunda representación teórica informática, centra su interés en precisar que es toda acción o conducta ilícita e ilegal, destinada, como lo señala Acurio (2016) a: “perturbar, desmejorar, devastar, o



maniobrar inescrupulosamente, un sistema basado en la informática o cualquiera de sus dispositivos, o con el fin, desde ella misma, producir lesiones o colocar en riesgo bienes de cualquier índole” (pág.14). La tercera de las ideas, la propone Parada (2016), quien, a pesar de simplificar su definición, denota un fuerte adeudo en la adaptación de los delincuentes a nuevas formas de delito, propios del avance de la informática.

A lo largo de la historia, el delito ha encontrado en la tecnología un aliado, toda vez que los delincuentes siempre han buscado innovar utilizando las herramientas y tecnología a su alcance para lograr sus objetivos. Denominaremos, “delito” a toda acción que así sea dispuesta por ley. Más concretamente, entenderemos como delito toda acción típica, antijurídica y culpable, siguiendo la doctrina clásica del derecho penal. (pág. 52),

Se cierra con la cuarta representación conceptual que determina Casabona, en Hernández (*ob.cit.*), quien:

...considera inadecuado el término “delito” porque tiene un

significado muy específico en Derecho penal que no se ajusta a algunas conductas clasificadas en ocasiones como delitos informáticos pero que no tienen su encuadre en ninguna conducta tipificada penalmente. Por eso acabará explicando que no puede hablarse de un único delito informático, sino de una pluralidad de ellos, en los que la única nota común es la vinculación de alguna manera con los ordenadores, sus funciones, el proceso y transferencia automatizada de datos, y la confección y/o utilización de programas para ello, sin que, sin embargo, sea el bien jurídico el mismo en todos los delitos informáticos ni presenten sus formas de comisión siempre las mismas características. (pág. 234).

### ***Pléyades jurídicas de la informática global***

Tras las generalidades de las definiciones de delitos informáticos, la amplitud de los desafíos legales nacionales e internacionales ocupan un sin número de aplicaciones de la informática en la vida diaria, haciendo de su ejercicio una esfera



transmoderna de difícil ejecución. En mundo global determinado por el auge de la superinformación, constituye un reto general en el uso de esa información, entendida como el derecho de firmas electrónicas, derecho de autor y producción intelectual, aspectos que nutren las garantías de la construcción del conocimiento, por lo cual, su tratamiento, ha de ser el mismo que se les da a las fuentes impresas, en las que prevalecen los derechos del autor o autores.

Este elemento determina un aspecto de gran relevancia, ya que la tendencia del internet, es que toda información se obtiene de forma real e inmediata, en ocasiones, las fuentes filtran documentos, datos y resultados de investigaciones, en la que su autor desconoce el tráfico, (Torres, 2015). Por ello, se debe ejercer un sistema jurídico que garantice la fluctuación de información, siempre en resguardo del derecho intelectual. De esta manera, se articula el libre proceso, el estado de derecho y garantías jurídicas a los internautas, así como a los e-intelectuales, comprendidos como aquellos que construyen conocimientos, lo difunden, socializan en los entornos online, potencializando el e-learnig.

Realidad que demanda procedimientos legales que den respuesta a un entorno interactivo, donde las comunidades crecen cada vez más, consolidando a la sociedad de

la información, en la que la data se encuentra directamente, composición que adquiere forma en la comunidad del aprendizaje y conocimiento, puesto que aquí se le da utilidad académica, social e intelectual a esa información, su provecho lo determina la finalidad de la acción que se emprenda. Sin embargo, existen principios moralmente dirigidos, donde la eticidad debe enmarcar las buenas costumbres en la noesis constructiva, pero los intereses personales, inoculan una lúgubre actitud deplorada de plagio, en la que no se refiere al autor original de la información utilizada.

Ante esta contundente vicisitud, el Estado Venezolano se ha guarecido para garantizar que el conocimiento dentro el espectro virtual o electrónico, siga expandiendo sus cimientos de cognición social, permitiendo que no se establezca como un nodo inactivo, sino como una dinamo interactiva. Es así, que la Ley sobre Mensajes de Datos y firmas Electrónicas (2000), en su Art. 5, establece: “los mensajes de datos estarán sometidos a las disposiciones constitucionales y legales que garantizan los derechos a la privacidad de las comunicaciones y de acceso a la información personal” (pág. 7).

Constituyéndose el marco legal de disposiciones electrónicas, donde las



personas se les garantizan el resguardo de la información que suministre en la web, sus mensajes personales y relación en las redes sociales, para lograr resguardo, protección y derecho de autoría ante la manifestación intelectual en todas sus dimensiones. Este recurso, es un medio de amparo común, donde las leyes no tienen limitación de acción, puesto que donde se genere acciones ciudadanas, el *ethos* jurídico tendrá cabida, claro está, que en el respeto de las jurisdicciones internacionales.

De tal manera que, el avance las tecnologías informáticas, y sus aplicaciones en casi la totalidad de las actividades sociales, económicas, laborales... tiene un resultado avasallante, al punto que, explícitas naciones se hallan en estado naciente en el plano jurídico sobre la materia, otras han enunciado cierto progreso, mientras que una imperceptible representación podría considerarse cuenta ya con un sistema legal consistente, trayendo consigo desigualdades que afectan la seguridad de los ciudadanos de la aldea global.

### ***Enfoques doctrinales jurídicos de la informática como escenario de delitos***

A partir de los enfoques doctrinales del derecho se divisan con propiedad teórica y

científica la multiplicidad de escenarios donde se presentan los delitos informáticos. Situación que solo muestra una arista dentro de un contexto colmado de grandes delitos, que por no mostrar rostros, entornos palpables, en ocasiones se desconoce los hechos punibles; es que los delitos informáticos dentro del espectro online, muestras acciones fraudulentas, entre las cuales resaltan las estafas económicas, donde existen personas que hackean información privada para sacar claves de cuentas bancarias y así despojar al usuario de sus pecunios, así mismo, realzan aquellas acciones en las que usurpan identidades de organizaciones o personas, para solicitar datos con los cuales puedan cometer el delito.

El cuidado de la información es imperativo para evitar estafas electrónicas, por cuanto el uso de las redes sociales ha de realizarse con conciencia de integridad personal, para que la información personal no sea de uso común, de esta manera se evitan secuestros exprés, online y telefónicos. Siendo estos, en los últimos años la tendencia de los delincuentes, “quienes como famosos pranes (reclusos con la mayor jerarquía de poder en un centro penitenciario), ejercen desde las cárceles” (Rodríguez, 2018). Constatándose que los delincuentes encuentran los medios para delinquir desde



la web, no ejercen tanto esfuerzo para lograr su cometido, ya que la víctima le facilita el proceso al dotarlo de la información necesaria y suficiente.

Al determinar semánticamente el uso de las redes sociales, es necesario conceptualizarla para tener una mejor comprensión gramatical del contexto escrito, a fin de establecer una lógica jurídica mediante los entornos electrónicos a los que se refiere, es por ello, que se definen dentro del internet, como aquellas interacciones entre usuarios, que se lleva a terminación a través de múltiples mecanismos que brinda la web 2.0, cuya intención central deviene de los intereses de las personas que interactúan, y las necesidades particulares de individualidades y/o grupos conectados en red. (Rico, 2012, 334).

Razón por la cual, es imprescindible hacer uso de las redes sociales y cualquier medio electrónico con cautela, para garantizar el bienestar e integridad desde la cotidianidad, por ser un entorno social de interacciones. Para ello, la persona ha de ser consciente del potencial de riesgo que son las redes sociales si se emplea sin juicio crítico, capaz de proyectar los peligros, beneficios y desventajas de los mismos. Sobre este entorno de realidades reparatorias, se sitúan los delitos de

violación de privacidad, donde las personas hacen uso de información personal de otros usuarios para desacreditarlos, estableciendo vilipendios y daños a la integridad de la buena moral de la persona. Su uso inadecuado constituye un elemento causal de procesos jurídicos. En este sentido, la Ley Especial contra los Delitos Informáticos (2001), en su artículo 6 determina: “Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa...”. (pág.4).

De esta manera, se establecen los procedimientos penados ante la ley, otorgándoles protección a las personas en todos los espacios de la ciudadanía, respetando los derechos humanos desde los entornos online. Aquí los principios y garantías de integridad, son procedimientos jurídicos que resguardan los derechos sociales a una vida plena. Su goce es el estamento jurídico para el adecuado comportamiento de las personas en los entornos virtuales, electrónicos, cuya tipificación comprenda los espacios electrónicos.

Estos procedimientos jurídicos son instancias legales para garantizar la libertad



de expresión sin menoscabo de su democratización, siempre en el marco de la justicia. Nunca puede ser asumido como un principio violatorio a la libertad, ya que ella establece los principios rectores, regula y orienta de manera responsable el uso de las redes sociales, la información personal, las garantías y derecho que representa cada persona en el contexto de una ciudadanía online; considerándose que el acto social no solo ha de ser una activación física interactiva, sino socializadora en cualquier medio electrónico.

### ***Riesgos informáticos (IT) cuantificados***

La alta variabilidad de riesgos informáticos que supone la tecnología para el ser humano y sus instituciones ha impactado la seguridad personal y empresarial, generando cierta susceptibilidad y suspicacia en el mundo global. Desde este contexto Cores (2019), describe que en la última década la tendencia de estafa electrónica ha crecido, pero desde esta pandemia ha cobrado gran empuje, ya que las personas han acrecentado el uso de la internet y las redes sociales. Los cuerpos de seguridad han presentado estadísticas de crecimiento de un 70% por delitos cometidos online. Es así, que los usuarios han de desarrollar una actitud de sigilo, cordura y resguardo ante

posibles amenazas, blindando su información al no difundirla como uso público.

Lo planteado por Cores (ob.cit), puede representar solo una pizca o apenas la punta del iceberg del impacto distorsionado de la informática para el fraude. Pero el asunto ocupa aún más espacio cuantitativo, pues para el año 2012, Malby indica que: “A nivel mundial, los actos delictivos cibernéticos muestran una distribución amplia... actualmente las estadísticas delictivas registradas por la policía no representan una base sólida para comparar los países, aunque dichas estadísticas son importantes para hacer políticas a nivel nacional”. (pág. 22).

En materia de derecho internacional, se encuentra el Principio de la universalidad y justicia mundial, el cual describe Acurio (2016) con precisión, como un principio que ha de aplicar el país que sea el primero en apresarse a un delincuente. Tendrá el beneficio práctico de cohibir delitos contra la humanidad catalogados como tal. Así pues, los convenios y acuerdos mundiales modernos aplican en cierta medida tal umbral. Sin embargo, es el mismo derecho penal, el que coloca una máxima en la aplicación de tal principio al considerar dos elementos: el primero sobre la calidad del bien y su elevación a intereses



supranacionales como es el caso del patrimonio común de la humanidad resguardado por la UNESCO, y el segundo, cuando el autor y/o autores del delito sean considerados de alta peligrosidad para los estados.

Esta visión amplía más el espectro de conocimiento sobre el fenómeno, pues fue una evaluación global impulsada por la ONU. Las razones obedecen a los actos delictivos cibernéticos de acuerdo a la tipificación de la ONU, son múltiples: orientadas a motivos financieros, difusión de contenidos informáticos violentos *few news* (noticias falsas/propias de las redes sociales de mensajería), acciones contra la privacidad de las personas: por vía de las encuestas aplicadas a las víctimas, erigieron estos datos con un macizo cotejo. Enuncia el estudio de la ONU, que los corolarios muestran que la victimización individual por causa de delitos cibernéticos, sobrepasan los delitos convencionales. Ahora obsérvese la realidad presentada:

Las tasas de victimización por fraude en línea con tarjetas de crédito, robo de identidad, respuesta a intentos de suplantación (phishing) y por experimentar acceso no autorizado a una cuenta de correo

varían entre el 1% y el 17% de la población con acceso a Internet de 21 países de todo el mundo, en comparación con tasas de robo, asalto y robo de coches de menos de 5 por ciento en los mismos países. Las tasas de victimización por delitos cibernéticos son más altas en los países con niveles menores de desarrollo, lo que destaca la necesidad de fortalecer los esfuerzos de prevención en esos países. (pág. 19).

En el año 2019, la ONU emite la resolución 73/187, denominada: “Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos”. La asamblea general de esta organización, requirió a los países miembros a presentar su balance en relación a las vicisitudes que afrontaban en la disputa contra el uso de las tecnologías de esta índole con fines delictuosos. En lo particular la voz oficial de Venezuela proporcionó la siguiente información: “...reconoció la creciente utilización de las tecnologías de la información y las comunicaciones y que el rol de la comunidad internacional en el uso de estas podría contribuir al logro de los objetivos de desarrollo acordados internacionalmente, incluidos los que



figuraban en la Agenda 2030 para el Desarrollo”. (pág. 90).

Pero además de las virtudes del uso de los medios informáticos Venezuela manifestó que: “...el uso ilícito de las tecnologías de la información y las comunicaciones podría tener un impacto perjudicial en la infraestructura, la seguridad nacional y el desarrollo económico de un Estado Miembro, por lo que puso énfasis en la necesidad de aumentar los esfuerzos internacionales para abordar ese problema”. Incluyó, además, que: “se pusiera fin al uso de las tecnologías de la información y las comunicaciones, incluidas las redes sociales, en contravención del derecho internacional y en detrimento de los intereses de los Estados Miembros”. (pág. 91).

La manifestación de las variantes de delitos informáticos por estafa y secuestro los recoge en su sitio oficial en internet la publicación digital del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), ente suscrito al Ministerio del Interior, Justicia y Paz de Venezuela, a través de las División Contra Secuestros y la División Contra Delitos Informáticos. Para el 1 de abril de 2021, expresa que se habrían registrado 31 casos de secuestros en la que va del año 2021 por ofertas publicadas por medio de la aplicación

Mercado, (aplicación creada por una red social multinacional, en el año 2007, dirigida a ofrecer la comercialización de productos y servicios).

La red social, opera en la totalidad de los países latinoamericanos, y según datos de la misma empresa, a nivel global un cuarto de sus usuarios, el equivalente a unos cuatrocientos millones hace uso de la aplicación citada. Destaca el CICPC, y su división respectiva que, la zona central del país conformada por los estados La Guaria, Miranda y el Distrito Capital, en El Valle, Petare y Coche son las áreas geográficas más propensas en este tipo de delitos, cometidos por bandas organizadas. En cuanto a estafas esta situación fue descrita por el citado cuerpo:

Una mujer dedicada a estafar por páginas electrónicas comerciales fue capturada en Caracas por detectives adscritos a la División Contra los Delitos Informáticos del CICPC. La detenida... quien ofrecía ropa, zapatos y teléfonos en páginas electrónicas de ventas por internet, luego de recibir el pago de los clientes, no entregaba los productos. Las pesquisas iniciaron las investigaciones de campo tras haber recibido



denuncias por parte de las víctimas, donde los funcionarios lograron identificar, ubicar y aprehender a la mujer... (pág. 1).

Indudablemente que no es la única persona dedicado a este tipo de delitos en Venezuela, donde el número de ciudadanos aprendidos por el modus operandi, es permanente cada semana. Por una parte, la minusvalía de los estados nación queda al descubierto, cuando del uso de redes informáticas trasnacionales se trata, dado que a pesar de que las mismas declaran expresamente estar apegadas a las normativas legales de los Estados Unidos de América, su uso particular delincencial en los países se ha vuelto sigiloso y de crecimiento exponencial. Frente a lo que Venezuela expuso ante la ONU en el 2019 que: "...en la actualidad los instrumentos internacionales de derecho penal para contrarrestar los delitos relacionados con las tecnologías de la información y las comunicaciones eran insuficientes..." (pág. 91).

Todo esto sin aún abordar lo referente a la vulnerabilidad de la intimidad de los ciudadanos. El contexto donde se desarrollan los delitos informáticos globales surge por el apresurado crecimiento de los usuarios en

las redes sociales, su inadecuado empleo y distribución, con respecto a esto García (2018), en su artículo de investigación, sobre la intimidad de las personas al usar redes sociales e internet. Concluyó, que las personas dan una importancia relativa a tener un perfil, pero lo ven muy útil para su vida, al ingresar a comunidades electrónicas como hecho de tendencia, lo cual, a arrastra a la mayoría de los adolescentes, jóvenes y adultos jóvenes a ser parte de dichas comunidades por modismo en las redes sociales.

Hallazgos que galopan una complejidad en la sociedad mundial, donde las tendencias, los modos, determinan el uso, apertura y comercialización de las redes sociales, sentido usual que garantizan las interacciones globales, aunado a la falta de orientación familiar, donde, en función a lo indicado por Cores, (2009) "existen millones de niños, niñas y adolescentes con perfiles sin ser supervisados por sus padres, madres; en ocasiones, estos desconocen en su totalidad dicha realidad" (pág. 23).

Aprestamiento que, por alta de roles y uso inadecuado de las redes sociales, se distorsiona el correcto empleo, dado que sus beneficios son más que las desventajas, puesto que estas han ayudado en la construcción intelectual, en la búsqueda de



delincuentes, en perdurar las realidades en contextos reales, escarificando casos desde el reencuentro de historias. Por lo tanto, el llamado es a desarrollar una conciencia en red, para que su empleo sean las garantías de derecho social.

### **Teleología del “*scelus*” informático**

Los fines que manifiestan los delincuentes con sus *scelus* (delitos) informáticos pueden clasificarse en función a la vulnerabilidad de las personas o usuarios, de acuerdo con Hernández (2009): “la integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos”. (pág.81).

Describe en su clasificación, Hernández (ob.cit) la Intimidad informática. De ésta se desprende el *habeas data* o autodeterminación informática, la cual exhorta a la protección frente a este género de conductas, teniendo principalmente, los bienes individuales, la intimidad e inviolabilidad informáticas, y como un nuevo cauce, el domicilio físico de cada persona. Una última interpretación, se corresponde a lo estructural-funcional de los sistemas informáticos, sobre los cuales se tiende a poner la plena confianza individual, familiar y/o corporativa. Detalla el autor al respecto:

En un sentido parecido se apunta como nuevo bien jurídico de carácter supraindividual característico de los delitos informáticos la confianza en el funcionamiento de los sistemas informatizados. Como ya se ha mencionado en relación a las propuestas que aluden a la idea de la seguridad informática, los delitos vinculados con la informática no sólo dañan en su comisión bienes jurídicos individuales y concretos; su comisión también pone en peligro la confianza de la sociedad en el buen funcionamiento de los sistemas informáticos y de las redes de transmisión de datos. La gravedad de este quebrantamiento de confianza radica, precisamente, en la dependencia de la sociedad actual respecto de las TICs para el desarrollo personal, económico y social de los individuos. (pág. 239).

### **Conclusiones**

Un desafío propio del siglo XXI está relacionado con la fuerte evolución digital global y las empresas que facilitan



herramientas de información para la comunicación y comercialización de productos, las cuales por su carácter transnacional generan una esfera de relatividades al momento de aplicar la norma en función de las transgresiones a las que puedan estar expuestos determinados personas, dada la despersonalización que caracteriza a tales empresas, y cuyas responsabilidades jurídicas solo se corresponden al país desde el cual operan, accesa la población mundial a una era de pléyades jurídicas de la informática global, cuyos límites son en cierta manera hasta desconocidos.

Otro desafío identificado en este ensayo, son las imprescindibles comprensiones y aplicaciones de los enfoques doctrinales jurídicos de la informática como escenario de delitos. Los países en vías de desarrollo, y de forma específica, Venezuela, han recalado la importancia de reducir las barreras para atenuar progresivamente los disímiles resquicios digitales, a través de un sólido tratamiento de las infracciones informáticas que limitan el avance de los sistemas y sus aplicaciones en línea, en el orden social, cultural y económico.

En cuanto a la cuantificación de los Riesgos Informáticos (IT), un representativo número de países aprecian que los centros

policiales para el manejo de datos sobre las infracciones informáticas a través de internet, no son asaces, pues una buena parte de estos no son reportados, o sus manejos no entran en correspondencia con el conocimiento de los imaginarios sociales propios de cada cultura. Este hecho se convierte en un ultimátum para la sociedad que ha de ser disipada desde la multidiversidad de escenarios institucionales y ciudadanos que ven amenazada su integridad por la inacción del sistema jurídico o por su tardía actuación, la cual facilita en muchos sentidos que se cometan los delitos de esta índole.

Además, en el mismo orden de ideas sobre la cuantificación y observación del delito informático, se hace preciso desarrollar en cada nación una labor que trascienda el dato meramente estadístico, y desvelar estratégicamente el ethos de los imaginarios sociales e individuales que subyacen en las realidades individuales y colectivas de los ciudadanos y ciudadanas en su imbricación con las labores apoyadas en el internet. Los aspectos más neurálgicos en cuanto a los retos jurídicos para el ethos humano en las plataformas digitales de internet, lo representan lo que se ha considerado en esta disertación como proximidad



gnoseológica jurídica sobre el “scelus” (delito) informático y su teleología. Pues, tanto las profundas diferencias sobre la norma entre las naciones, a lo que se le suma la carencia de principios conducentes a la unificación de cláusulas, concepciones y términos, los cuales hacen más compleja la situación, dado el grado de desigualdad en la implementación de la informática, redes y sus aplicaciones en los países. Ello se traduce en la imperiosa unificación de la norma en diversos niveles geopolíticos, teniendo como punto de inicio la formulación unificada de tipificaciones del delito de este tipo en cada país y posteriormente en las regiones continentales. Y, por último, la tipificación disímil en las naciones y/o hasta inexistente crea las bases para el desborde del quebrantamiento de la norma de forma sigilosa conduciendo a una peligrosa ignominia digital.

#### REFERENCIAS

Acurio, S. (2016). *Delitos Informáticos: Generalidades*. España.

CICPC. (2021). *Reporte de delitos informáticos*. [Sitio web en línea]. Disponible en: <https://revistacicpc.com/cicpc-delitos-informaticos>. [Consulta: 2021, marzo 30].

Cores, H. (2019). *Privacidad e intimidad en las redes sociales*. [Documento en línea]. Disponible: <https://reunir.unir.net/>. [Consulta: 2021, marzo 01].

García, J. (2018). *Estudio sobre la privacidad en el uso de las redes sociales de internet*. Trabajo e Grado, Universidad Nacional de México. México D. F.

Hernández, L. (2009). *El Delito Informático*. Eguzkilore: San Sebastián.

*Ley Especial contra los Delitos Informáticos* (2001). Gaceta Oficial N.º 37.313, Extraordinario, de fecha 30 de octubre de 2000.

*Ley sobre Mensajes de Datos y firmas Electrónicas* (2000). Gaceta Oficial N.º 37.076, Extraordinario, de fecha 13 de diciembre de 2000.

Malby, S., Mace, R., Holterhof, A., Brown, B., Kascherus, S. y Ignatuschtschenko, E. (2012). *Estudio exhaustivo sobre el delito cibernético: Organización de las Naciones Unidas*. UNODC: Nueva York

Organización de las Naciones Unidas. (2019). Septuagésimo cuarto período de sesiones Tema 109 del programa provisional: *Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos*. Nueva York: EUA.



- Parada, R. y Errecaborde, D. (2018). *Ciberdelincuencia y delitos informáticos: los nuevos tipos penales en la era de internet*. Ciudad Autónoma de Buenos Aires: Erreius.
- Rico, M. (2012). *El impacto de internet y las redes sociales en el derecho a la libertad de expresión*. Universidad del Zulia: Revista Fronesis.
- Rodríguez, G. (2018). *En contraste*. [Documento en línea]. Disponible: <https://eluniversal.com> [Consulta: 2020, marzo 30].
- Torres, G. (2015). *Tecnología de la información y comunicación*. España: McGraw Hill.
- Delgado, D; Urgilés, D; Vega, P. (2020). *Ahora vienen los Z: Una Generación de nuevos Ciudadanos*. *Revista Científica*, 5 (16), 290-304, e-ISSN: 2542-2987.