Perspectiva criminológica y dogmática de los de los delitos relacionados con el bien jurídico de la información y de los datos.

Estudiante
Juan José Ospina Grajales

Director
Enan Arrieta Burgos

Trabajo presentado como requisito parcial para optar al título de abogado

Pregrado en Derecho

Escuela de Derecho y Ciencias Políticas

Universidad Pontificia Bolivariana

Medellín

2021

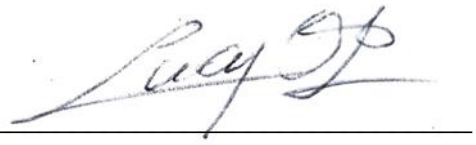
Declaración de originalidad

Fecha: 18 de mayo de 2021

Juan José Ospina Grajales

Declaro que este trabajo de grado no ha sido presentado con anterioridad para optar a un título, ya sea en igual forma o con variaciones, en esta o en cualquiera otra universidad.

Declaro, asimismo, que he respetado los derechos de autor y he hecho uso correcto de las normas de citación de fuentes, con base en lo dispuesto en las normas de publicación previstas en los reglamentos de la Universidad.



_____

Perspectiva criminológica y dogmática de los delitos relacionados con el bien jurídico de la información y de los datos

Resumen

En este trabajo se analizan los tipos penales creados a través de la Ley 1273 de 2009 que pretenden proteger el bien jurídico de la información y de los datos. El objetivo es descubrir las razones de criminalización primaria, así como establecer la estructura dogmática elemental de las conductas descritas en los tipos penales aludidos. La conclusión será que estas conductas, en síntesis, fueron criminalizadas producto del feroz avance de la informática y que los tipos penales que las consagran son, por regla general, básicos, de conducta alternativa, de mera conducta, abiertos, de sujeto activo común, pluriofensivos, comisivos y dolosos. La metodología consistirá en aproximarse a la Ley 1273 de 2009 y a la jurisprudencia atinente, primero en clave criminológica y luego dogmática, para en ultimas valorar la eficacia de esta regulación. Previo a lo anterior, se introducirá el tema aclarando conceptos comunes y formulando el problema de investigación que se pretenderá resolver a lo largo del trabajo.

Palabras clave. A27
Criminología, dogmática penal, tipo penal, ciberdelito.

Introducción

Según un informe publicado por la Escuela Técnica Superior de Ingeniería Informática de la Universidad Politécnica de Valencia (2016), el surgimiento de la informática se remonta a la Segunda Guerra Mundial cuando se crea, para descifrar la máquina de encriptación de mensajes entre alemanes, el primer modelo (mecánico) de ordenador, denominado Colossus y atribuido al matemático Allan Turing. Este era utilizado con fines exclusivamente militares o científicos. Solo hasta 1952 se producen los primeros ordenadores comerciales (Universidad Politécnica de Valencia, op. cit., pág. 17). Entre 1964 y 1971, se logran disminuir el costo de producción y el gran tamaño de estas máquinas, por virtud del desarrollo de los circuitos integrados (Universidad Politécnica de Valencia, loc. cit.). En 1981 surgen los microprocesadores, la piedra angular de los computadores que actualmente se conocen (Universidad Politécnica de Valencia, loc. cit.). Cabe aclarar que, según aquel informe, antes del siglo XX ya existían prototipos de procesamiento de datos, como la Tabuladora de Hollerith o la Maquina de

diferencias de Babbage, pero el antecedente más inmediato y relevante de la informática se encuentra en el periodo histórico ya referido (Universidad Politécnica de Valencia, loc. cit.).

La informática es un pilar del progreso social, posibilitando tareas que para un humano serían imposibles sin ella. Piénsese, por ejemplo, en cómo se llevaría a cabo un viaje espacial o una comunicación transoceánica sin un avanzado servidor de datos. No obstante, y desgraciadamente, la informática es también caldo de cultivo para criminales: pueden estos obtener, interceptar o sustraer información confidencial, transferirse activos ajenos, espiar, suplantar, sabotear, hurtar u otros, sin necesidad de desplazar su cuerpo de un sitio determinado y, en ese sentido, sin tener que revelar su identidad. ¿Acaso puede haber un ambiente más propicio para la impunidad? La situación anterior se agrava si se estima que casi toda persona, empresa o Estado en el mundo, consecuencia de la globalización, hace uso de un sistema informático para almacenar información o activos.

El Estado colombiano no está exento y es consciente de la presencia de criminales que se valen de medios informáticos para cometer ilícitos. Por ello, en 2009 el Congreso creó y promulgó la Ley 1273, por medio de la cual se modificó el Código Penal, creando un nuevo bien jurídico-penal denominado "de la protección de la información y de los datos". Esta Ley, como todas, fue objeto de una serie de debates sucesivos e intercalados entre Senado y Cámara, en los cuales se determinó por qué debían introducirse once nuevos tipos penales en el ordenamiento jurídico.

En criminología, al por qué el legislador prohíbe lo que antes consideraba una simple conducta desviada, se le denomina criminalización primaria. En dogmática, los tipos penales pueden clasificarse en atención a múltiples criterios. Entonces, como se podría avizorar, este trabajo apunta a establecer (i) cuáles son las causas de criminalización primaria de los delitos relacionados con el bien jurídico de la información y de los datos y (ii) cómo se clasifican dogmáticamente los tipos penales que los consagran.

Este trabajo se justifica en tanto contribuye al progreso de los saberes penales que hacen énfasis en la dimensión fáctica y normativa del fenómeno criminal. En sede de la expansión inexorable de la informática, adquiere importancia conocer, íntegramente, aquellos delitos que se ejecutan echando mano de ésta. Quien pretenda ser un prominente penalista debe comprender, no sólo las clásicas figuras delictivas, como el hurto o el homicidio, sino también las que surgen con

ocasión del progreso, como el Uso de software malicioso (Ley 1273, 2009, art. 269E) o el Hurto por medios informáticos" (loc. cit., art. 269I), bien para enervar efectivamente la pretensión punitiva del ente acusador, en el caso del abogado defensor, bien para sacar avante la acusación realizada, en el caso del fiscal.

En concordancia con el problema de investigación, se concluirán dos cosas: (i) que las conductas consagradas en la Ley 1273 de 2009 fueron criminalizadas debido a un incremento masivo del uso de sistemas informáticos y al correlativo surgimiento de una nueva categoría de criminales; y (ii) que los tipos penales que consagran dichas conductas son, por regla general, básicos, de conducta alternativa, de mera conducta, abiertos, de sujeto activo común, pluriofensivos, comisivos y dolosos.

Para los efectos anteriormente descritos, en el primer capítulo se analizarán los debates del proyecto de Ley 1273 de 2009; en el segundo, se clasificaran dogmáticamente los tipos penales creados a través aquella; en el tercero y último, se valorara el impacto que ha tenido la regulación penal de los ciberdelitos.

1. Aproximación Criminológica y Político Criminal a la Ley 1273 de 2009

Para aproximarse político criminal y criminológicamente a una ley, debemos entender cómo se relacionan estos dos conceptos: criminología y ley. Por tanto, en este capítulo se hablará del derecho objetivo y sus fuentes haciendo especial énfasis en la ley, para desembocar en el proceso legislativo, se definirá qué es la criminología, se ahondará en lo que se denomina criminalización primaria y su diferencia con la política criminal, y en ultimas se analizaran los debates del proyecto de Ley 1273.

El derecho puede ser entendido en, al menos, cinco sentidos (Solano, 2016). Hablemos de las las tres acepciones más comunes: el derecho en sentido objetivo, referido al conjunto de normas que imponen deberes o conceden facultades o, lo que es lo mismo, de preceptos imperativos atributivos (Máynes, 2002, p. 36); el derecho en sentido subjetivo, referido a aquel deber o facultad derivado de la norma (Máynes, loc. cit); el derecho en sentido cientifico, referido al estudio del derecho objetivo (Solano, loc. cit.).

Centremos el análisis en aquel conjunto de normas que imponen deberes o conceden facultades. El derecho objetivo es susceptible de clasificarse en derecho positivo y derecho natural. El derecho positivo es "el que efectivamente se cumple en una determinada sociedad y una cierta época" (Máynez, op. cit., p. 40). El derecho natural es el "que existe al lado o por encima del positivo" (Máynez, loc. cit.). El positivismo jurídico dirá que esta clasificación es improcedente en tanto derecho objetivo no es más que un sinónimo de derecho positivo. No se disertará sobre esta disputa, entre positivistas y naturalistas, que ríos de tinta ha hecho correr.

El derecho objetivo, o como diría Kelsen (1994), ese conjunto de pensamientos imperativos objetivados, puede tener diversas fuentes. En este punto, el doctor Solano (op. cit., p. 144-145) propone una distinción valiosa para este trabajo entre fuentes formales, referidas al proceso de producción de la norma; materiales, referidas a los hechos determinantes de creación y contenido de la norma; de producción, referidas a la autoridad creadora de la norma; y de manifestación, referidas a la forma de expresión de la norma. Esta distinción es valiosa en tanto permite afirmar que lo que aquí se denomina fuente material del derecho en criminología, como veremos, se denomina causas de criminalización primaria. Echando mano de lo anterior, digamos que la ley, la jurisprudencia y la doctrina, arquetipos de fuentes de derecho, son, en rigor, simples fuentes de manifestación del derecho.

La ley es un conjunto de enunciados normativos por vía de los cuales se expresan normas que versan sobre una misma materia (Solano, loc. cit.). La fuente formal de la ley es el proceso legislativo. El proceso legislativo, someramente, consta de una iniciativa legislativa, de la asignación de un ponente, de cuatro debates, de una sanción o de una (s) objeción presidencial y de una promulgación. El primer paso del proceso legislativo puede ser dado por un congresista o su bancada, el Gobierno, el 5% de los ciudadanos del censo electoral, el 35% de los concejales o diputados, las Altas Cortes y organismos de control y electorales. Ese primer paso obedece a una necesidad: regular un fenómeno social o regular un fenómeno criminal.

El fenómeno criminal, como todo fenómeno jurídico según Reale (1993), es susceptible de ser analizado desde tres dimensiones o perspectivas: normativa, valorativa y fáctica. El fenómeno criminal, como afirma Baquerizo (1991) en igual sentido, es el conjunto tres realidades:

jurídica, social e individual. Ahora bien, hay saberes[1] que estudian dichas dimensiones o realidades: la dogmática jurídico penal se ocupa de la dimensión normativa o jurídica, la política criminal de la valorativa o social y la criminología de la fáctica a nivel individual y social.

La política criminal es la acción del Estado en contra el crimen (Liszt, 1999), es el

> Saber penal que se pregunta por los fines que la pena debe cumplir en la sociedad, por cómo deben redactarse las leyes penales, cómo deben construirse los tipos penales, cuáles deben ser las sanciones aplicables, cuál debe ser la magnitud de tales sanciones, cuáles expectativas sociales deben ser protegidas por el derecho penal y, más aún, cuáles no. (Solano et al, op. cit.)

La criminología es una

> Ciencia empírica e interdisciplinaria, que se ocupa del delito, el delincuente, la víctima y el control social del comportamiento delictivo; y que trata de suministrar una información válida, asegurada, sobre la génesis y dinámica del problema criminal y sus variables; sobre los programas y estrategias de prevención eficaz del delito; y sobre las técnicas de intervención positiva en el hombre delincuente". (García-Pablos, 1989, p. 79-94)

La criminología es una "ciencia del crimen o estudio científico de la criminalidad, sus causas y medios para combatirla" (Manzanera, 1981, p. 15). El objeto de estudio de la criminología lo constituyen los factores de criminalidad y criminalización (Conde y García Arán, 2010).

Vistas las definiciones, podemos afirmar que la criminología informa a la política criminal de la existencia de un fenómeno criminal y sus causas y del catálogo de medios de los que dispone para hacerle frente, con miras a que esta escoja uno (s) y lo configure de tal forma que sea eficaz. Existe entre estos dos saberes una relación de complementariedad. Tanto así que Franz von Liszt propuso en 1889 (p. 452) la creación de una ciencia del derecho penal integrada

[1]Se prefiere la expresión "saberes penales" sin que ello implique la negación o afirmación del carácter científico del derecho penal.

(“*gesamte strafrechtswissenschaf”*) en la que, al lado del estudio de las normas, hubiese un estudio de las causas del delito y la eficacia de la pena con miras a lograr una lucha eficaz contra el crimen.

La criminología y la política criminal, como se evidenció, son saberes totalmente independientes, con un objeto y un método de estudio propio, sin embargo, en sede de un concepto propio de la primera parece difuminarse el lindero que las distingue. Nos referimos a la criminalización primaria. Veremos en seguida que se denomina así a una labor perteneciente a la política criminal: legislar penalmente.

La criminalización primaria, siguiendo a Zaffaroni et al. (2002, p. 11), puede definirse como la “formalización penal de una conducta en una ley”. Lo hace la respectiva agencia legislativa definiendo en abstracto quienes serán los seleccionables para ingresar en el sistema penal. La criminalización primaria, como casi toda decisión humana, obedece a un por qué y a un para qué. Diría Zaffaroni (op. cit.) que el por qué gira en torno a la idea de estereotipo y vulnerabilidad. Diremos nosotros que en el contexto de la Ley 1273 de 2009 esto no es cierto, pues los ciberdelincuentes difícilmente se pueden encajar en algún estereotipo, dado que actúan desde el anonimato, y en ese sentido su vulnerabilidad es poca. Adentrémonos, pues, en el análisis criminológico de las conductas contenidas en la citada ley, o digamos también, en el análisis de la fuente material de esta.

Para cumplir el propósito planteado podemos empezar ubicando los principales antecedentes históricos normativos, nacionales e internacionales, de la Ley 1273 de 2009.

- Convenio de Budapest de 2001: creado por la necesidad de llevar a cabo, con prioridad, una política penal común destinada a prevenir la criminalidad en el ciberespacio. Colombia se adhirió a este solo hasta hace tres años, ratificándolo a través de la Ley 1928 de 2018.

- Decisión Marco 222 de 2005: emitida por el Consejo de la Unión Europea para reforzar la cooperación entre las autoridades judiciales y otras autoridades competentes, mediante la aproximación a su legislación penal en materia de ataques contra los sistemas de información.

- Decreto 1360 de 1989: reglamenta la inscripción de software en el Registro Nacional del Derecho de Autor para proteger la propiedad intelectual informática.

- Decreto 100 de 1980: consagraba en su artículo 195 el delito de Acceso Abusivo a un Sistema Informático, en los mismos términos que veremos mas adelante. Este tipo cayó en desuso porque consagraba como consecuencia jurídica la multa.

Hasta aquí hemos visto que la comunidad internacional creó una regulación de los delitos informáticos, la cual solo acogieron, en principio, países europeos. Esta regulación, se cree, surgió producto de la propagación de gusanos[2] y virus informáticos y del ataque cibernético que sufrió en 1999 el Departamento de Defensa de Estados Unidos y la Administración Nacional de Aeronáutica y del Espacio (NASA). A Colombia, los ataques y desfalcos cibernéticos la compelieron a buscar una solución, aunque fue tardía y lenta en comparación al resto del mundo.

- Proyecto de Ley 42 de 2007: pretendía agravar las penas de los delitos de hurto calificado, daño en bien ajeno, violación de reserva industrial o comercial, cuando se cometieran vulnerando la seguridad informática de las víctimas o valiéndose de sistemas informáticos.

- Proyecto de Ley 123 de 2007: buscaba la inclusión de un nuevo título en el Código Penal y, correlativamente, la creación de un bien jurídico independiente. Elaborado por el ex juez Alexander y por los doctrinantes Fernando Velásquez Velásquez, Jarvey Rincón y Gabriel Roldan.

En últimas, se acogió mayormente la propuesta del proyecto 123 y, por ende, se eligió el sistema legislativo consistente en confeccionar un título adicional para ser incluido en el estatuto punitivo, porque si bien era más técnica la expedición de una ley especial, ella podría perderse

[2] Un gusano informático es un malware que se replica para propagarse a otras computadoras.

> Dentro de todo el entramado del ordenamiento jurídico, sin merecer la atención requerida por parte de estudiosos y administradores de justicia, quienes, pretextando dificultades técnicas, falta de preparación, etc., prefieren dejar en el olvido este tipo de normatividades que terminan por no ser aplicadas o, si lo son, de una manera deficiente. (Primera ponencia del proyecto de ley 1273, Cámara, 2008)

El método que se venía dando por el legislador resultaba escaso para salvaguardar la información y los datos informáticos, pues dejaba vacíos que comportaban su vulneración. En palabras de Becharla et al. (2020), el amparo de este bien jurídico no podía darse de manera indirecta por otros tipos penales, o como agravante, sino que necesitaba de la creación de tipos penales autónomos, donde el fin principal fuese este bien y así su tutela resultara más eficaz

Como se dijo, el proyecto sugería la creación de un título y dos capítulos. Esto se acogió de la siguiente forma: el primer capítulo agrupa las conductas tratadas en el Convenio de Budapest y las que atentan contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; el segundo agrupa las conductas que atentan contra el tráfico informático y otros intereses jurídicos.

Se podría pensar que la ley bajo análisis protege un único bien jurídico: la información y los datos. No obstante, las ponencias referidas al Hurto por medios informáticos y semejantes y a la Transferencia no consentida de activos precisan que el primero procura "completar las descripciones típicas contenidas en los artículos 239 y siguientes del Código Penal, a las cuales se remite expresamente" y el segundo busca variar la estafa clásica por la figura de la estafa electrónica (Segunda ponencia del proyecto de ley 1773, Cámara, 2007).

Finalmente, el proyecto lograría su sanción presidencial el 5 de enero de 2009 para derivar en la expedición de la denominada Ley de delitos informáticos 1273 de 2009.

Ahora bien, la iniciativa legislativa del congresista Germán Varón Cotrino surge porque, parafraseando a Pérez et al. (2010), el uso de internet se había extendido y había aumentado el riesgo de su uso inadecuado. Los delincuentes cibernéticos viajaban por el mundo virtual y realizaban incursiones fraudulentas cada vez más frecuentes y variadas. Sus herramientas habían evolucionado a pasos agigantados. En un comienzo, en igual sentido de Pérez et al. (loc. cit.), infectaban los equipos de sus víctimas al transportar mano a mano los virus desarrollados,

en los medios de almacenamiento de información disponibles en ese momento: los disquetes. Más tarde, utilizaron las redes de datos al aprovechar la internet, pero se toparon con restricciones de acceso para evitar contagios. En ultimas, regresarían a la difusión contaminante mano a mano y los bombardeos de malware. Nada de esto acarreaba, ni en la práctica ni en la teoría, consecuencias jurídicas.

La necesidad de una ley de delitos informáticos emanó entonces de la existencia de personas que utilizaban su talento y conocimiento de los sistemas informáticos para tratar de sacar provecho de ello en detrimento de sus semejantes, recurriendo a conductas que, por lo novedosas, o no se encontraban tipificadas o su sanción tenía una relativa dificultad pues la adecuación típica no era lo suficientemente clara. Se buscaba con el proyecto la creación de un decálogo de tipos penales dado que "el aprovechamiento de condiciones, talentos y conocimientos privilegiados, propios de la comisión de delitos valiéndose de medios informáticos o sobre medios informáticos, implica una especial censura por la correlativa indefensión de la mayoría de los usuarios. (Exposición de motivos, 2007).

2. Clasificación Dogmática de los Tipos Penales Creados con la Ley 1273 de 2009

Para hablar de clasificación de tipos penales responsablemente, debemos recorrer un camino conceptual que vaya desde la dogmática penal a la tipicidad. Por tanto, en este capítulo se definirá qué es la dogmática jurídico penal y la teoría del delito, se precisará cuáles son las categorías dogmáticas del delito, se ahondará en la tipicidad y en el concepto de tipo penal, y en ultimas se analizarán los tipos penales de la Ley 1273 de 2009.

El derecho penal puede ser entendido en tres sentidos: el derecho penal en sentido objetivo o *ius poenale*, referido al "conjunto de normas jurídicas que al delito como presupuesto asocian penas y (o) medidas de seguridad como consecuencia jurídica" (Bockelmann, 1975, como se citó en Mir Puig, 2003, p. 7); el derecho penal en sentido subjetivo o *ius puniendi*, referido a la "potestad punitiva" radicada en cabeza del estado (Olivares, 1976, p. 37); y el derecho penal en sentido científico o dogmático, referido al "estudio del derecho penal en sentido objetivo" (Velásquez, 2020, p. 5)

Interesa, especialmente, profundizar en la última acepción. El derecho penal en sentido científico o dogmático es un saber que se ocupa de estudiar sistemáticamente el derecho penal objetivo o positivo, en su parte general o especial, con miras a limitar el ejercicio del poder punitivo del estado. Es a lo anterior a lo que técnicamente se le denomina dogmática jurídico penal.

En el sentido de Solano et al. (op. cit.), como ya se anticipó, la dogmática jurídico penal hace parte de un conjunto disciplinas que se encargan de examinar el fenómeno criminal desde distintas perspectivas. La dogmática estudia el fenómeno criminal desde la perspectiva normativa. La política criminal y la criminología, por su parte, estudian aquel fenómeno desde las perspectivas valorativa y fáctica, respectivamente. La política criminal, en síntesis, establece cómo debería el estado hacerle frente a los delitos, mientras que la criminología estudia el porqué de estos.

La dogmática jurídico penal, se dijo, estudia el derecho penal objetivo o positivo, en su parte general y especial. Cuando aquella estudia la parte general de este pretende responder tres interrogantes: 1. ¿Qué es el derecho penal?; 2. ¿Qué es la conducta punible?; 3. ¿Cuáles son las consecuencias derivadas de la conducta punible? Al efecto se formulan tres teorías: 1. Teoría general del derecho penal; 2. Teoría general del delito; 3. Teoría general de la responsabilidad penal.

Vamos a centrarnos un poco en la teoría formulada para responder qué es la conducta punible. La teoría general del delito sistematiza los elementos son comunes a todos los delitos de un determinado derecho positivo (autor, participe, dolo, culpa, acción, omisión, etc.). Los teóricos, incluso, han definido qué se entiende por delito, en aras de delimitar sus componentes esenciales y así excluir del ejercicio del poder punitivo los fenómenos o conductas que no los reúnan. Francesco Carrara (1971) lo definía como "la infracción a la ley del Estado, promulgada para proteger la seguridad de los ciudadanos que resulta de un acto externo del hombre, positivo o negativo, moralmente imputable y socialmente dañoso" (p. 60). Enrico Ferri (1993) lo definía como "la ofensa de un hombre a otro violando un derecho o un bien que se concreta en la persona o en la cosa mediante una acción psíquica que termina y guía una acción física, produciendo un daño público y privado" (p. 20). Raffaele Garofalo (1885) lo definía como "la lesión de aquella parte de los sentimientos altruistas fundamentales de piedad o probidad, en la medida en que son poseídos por una comunidad, y que es indispensable para la

adaptación del individuo a la sociedad" (p. 160). Ernst von Beling (1994), positivista alemán del siglo XIX, fue el primero en definirlo como una "acción típicamente antijurídica y correspondientemente culpable" (p. 29). Este concepto fue acogido, con matices, por nuestro legislador[3]. El delito así concebido consta de cuatro "categorías dogmáticas" ordenadas lógicamente: conducta, tipicidad, antijuridicidad y culpabilidad. Las categorías dogmáticas constituyen filtros al ejercicio irracional del poder punitivo, pues "no se trata de que pase cualquier agua ni en cualquier forma, sino que su cantidad, calidad y forma de paso deben ser predeterminadas inteligentemente" (Zaffaroni et al., op. cit., p. 291). Hablemos sucintamente de cada una de ellas, definiéndolas y señalando sus causales de exclusión y los principios que proyectan, dejando la tipicidad al final por efectos prácticos.

Conducta es un comportamiento humano controlado y dirigido por la voluntad que "produce una mutación en el mundo exterior" (Mahecha, 1963) . Si se trata de un hecho de la naturaleza, de un animal o de una persona jurídica, no habrá conducta por cuanto no hay comportamiento humano. Si se trata de un hecho cometido producto de *vis maior*[4], de un acto reflejo o de un estado de plena conciencia, no habrá conducta por cuanto no hay comportamiento humano controlado y dirigido por la voluntad. Si se trata de un pensamiento que no trasciende al mundo exterior, no habrá conducta por cuanto ni siquiera se exteriorizó la voluntad. La conducta materializa el principio del acto o de la objetividad material, por lo cual, si no hay conducta no habrá delito.

Antijuridicidad es un juicio de desvalor que recae sobre una conducta por haber esta lesionado o puesto en peligro, sin justa causa, el bien jurídico protegido por vía del tipo penal. Von Liszt (1911), como se citó en Mir Puig (1994, p. 5), fue el primero en distinguir entre antijuridicidad material y formal, siendo aquella lo ya dicho y está la "infracción de una norma estatal, de un mandato o prohibición del ordenamiento jurídico".

Si la conducta no lesiona o pone en peligro el bien jurídico, no habrá antijuridicidad material. Si la conducta lesiona o pone en peligro el bien jurídico, pero media una causal de justificación[5], como legítima defensa, consentimiento del sujeto pasivo o estado de necesidad

[3] "Para que la conducta sea punible se requiere que sea típica, antijurídica y culpable. La causalidad por sí sola no basta para la imputación jurídica del resultado" (Ley 599, 2000, art. 9)
[4] *Vis maior* es una locución latina que significa fuerza mayor.
[5] Una "causal de justificación recorta por vía general el ámbito de la prohibición típica, integra en realidad cada figura delictiva, la delimita negativamente" (Carrasquilla, 1982, p. 391- 475)

justificante, no habrá antijuridicidad formal. La antijuridicidad materializa el principio de lesividad y de proporcionalidad, por lo cual, si no hay daño o el sacrificio de la norma comporta mayores ventajas que el daño, no habrá delito.

Culpabilidad es un juicio de desvalor que recae, ya no estrictamente sobre la conducta sino sobre el sujeto que la realizó, por haber este realizado un injusto siéndole jurídicamente exigible que no lo realizara. "Culpabilidad significa que son objeto de valoración negativa las máximas por las que se ha dejado llevar el autor en la formación de la voluntad y que, por ello, le puede ser reprochado personalmente el hecho" (Jescheck, 1996, p. 597). Si la conducta se realiza en un error de prohibición invencible o en un estado de necesidad exculpante o si la realiza un inimputable[6], no habrá culpabilidad. La culpabilidad materializa el principio de culpabilidad, por lo cual, si el hecho no se encuentra vinculado al autor a título de dolo, culpa o preterintención, no habrá delito.

Tipicidad es un juicio de desvalor que recae sobre la conducta por "su coincidencia o adecuación a las características imaginadas por el legislador, esto es, al tipo penal" (Velásquez, op. cit., p. 346). Si la conducta se realiza en un error de tipo, en cualquiera de sus formas, no habrá tipicidad. La tipicidad materializa, entre otros, el principio de legalidad, por lo cual, si no existe una ley previa, escrita, estricta y cierta, no habrá delito. El tipo penal, como se advierte, es el elemento nuclear de la categoría de la tipicidad. La expresión tipo proviene de la expresión latina *tipus* que significa "imagen o modelo de algo". El tipo penal es, pues, la descripción hecha por el legislador de una conducta, tanto en su aspecto objetivo como en su aspecto subjetivo, con miras a prohibirla, ordenarla o prescribir la observancia del deber de cuidado (Solano et al., op. cit., p. 67). El tipo penal, dicen Zaffaroni et al, "es la fórmula legal necesaria al poder punitivo para habilitar su ejercicio formal, y al derecho penal para reducir las hipótesis de pragmas conflictivos y para valorar limitativamente la prohibición penal de las acciones sometidas a decisión jurídica" (op. cit., p. 341)

Los tipos penales son susceptibles de multiplicidad de clasificaciones en atención a diversidad criterios. Acá precisaremos la clasificación que se hace en atención su estructura, a la conducta en ellos descrita, al sujeto activo de la conducta en ellos descrita, al bien jurídico y a la forma

[6] En el caso de los inimputables sí hay delito, pero no se impondrá una pena, sino una medida de seguridad, a título de consecuencia jurídica.

de individualización de la conducta. Después de esto, pasaremos a reflexionar sobre cada uno de los tipos penales que trae la Ley 1273 de 2009.

En lo subsiguiente, seguiremos la clasificación propuesta por el profesor Fernando Velásquez Velásquez en su libro Fundamentos de Derecho Penal (p. 408-214)

Los tipos penales, en atención a su estructura, se clasifican en:

- Tipos fundamentales: aquellos que describen una o varias conductas sin sujeción a ningún otro tipo penal
- Tipos subordinados: aquellos que, refiriéndose a un tipo básico o fundamental, le agregan elementos que lo modifican.
- Tipos autónomos: aquellos que reproducen la conducta de un tipo básico fundamental, pero le agregan elementos que lo modifican.

Los tipos penales, en atención a la conducta en ellos descrita, se clasifican en:

- Tipos elementales o entornos: aquellos que describen una sola conducta, concretada por medio de un solo verbo rector
- Tipos compuestos: aquellos que describen varias conductas.
    - Compuestos mixtos o de conducta alternativa: aquellos que describen varias conductas, pero con la realización de cualquiera de ellas se entiende consumada la conducta típica.
    - Compuestos complejos: aquellos que describen varias conductas que, al ser apreciadas por separado darían lugar a distintas tipicidades distintas, pero el legislador ha agrupado todas esas conductas creando un tipo penal independiente.

- Tipos de mera conducta: aquellos que no individualizan una determinada modificación en el mundo exterior que deba seguirse de la realización de la conducta en ellos descrita.
- Tipos de resultado material: aquellos que individualizan una determinada modificación en el mundo exterior, espacio-temporalmente separada de la conducta, que debe seguirse de la realización de ésta.

- Tipos abiertos: aquellos que no individualizan en forma precisa la conducta en ellos descrita. Estos utilizan expresiones con un contenido semántico amplio y de relativa vaguedad (Corte Constitucional, C-091, 2017)
- Tipos cerrados: aquellos que individualizan en forma precisa la conducta en ellos descrita.

Los tipos penales, en atención al sujeto activo de la conducta en ellos descrita, se clasifican en:

- Tipos de sujeto activo común: aquellos que no exigen una determinada calidad para el sujeto activo de la conducta en ellos descrita.
- Tipos de sujeto activo calificado: aquellos que exigen una determinada calidad especial para el sujeto activo de la conducta en ellos descrita.

Los tipos penales, en atención al bien jurídico protegido, se clasifican en:

- Tipos monofensivos: aquellos que describen una o varias conductas susceptibles de afectar un solo bien jurídico.
- Tipos pluriofensivos: aquellos que describen una o varias conductas susceptibles de afectar varios bienes jurídicos.

Los tipos penales, en atención a la forma de individualización de la conducta, se clasifican en:

- Tipos comisivos: aquellos que describen la acción prohibida.
- Tipos omisivos: aquellos que describen la acción ordenada.

- Tipos dolosos: aquellos que individualizan la conducta atendiendo a su finalidad en si misma considerada.
- Tipos culposos: aquellos que individualizan la conducta, no atendiendo a su finalidad en si misma considerada, sino atendiendo a la particular forma de exteriorización de dicha finalidad.

Todas estas categorías, al no ser excluyentes entre sí, pueden estar presentes en un mismo tipo penal. Por ejemplo, el tipo de homicidio simple es fundamental, elemental, de resultado, material, cerrado, de sujeto activo común, monofensivo, comisivo y doloso.

Como nos propusimos, trasegamos de la dogmática a la tipicidad y al tipo penal, pasando por la teoría del delito y las categorías dogmáticas. Ahora sí corresponde sistematizar los once tipos penales que trae la Ley 1273 de 2009. Digamos desde ya que absolutamente todos, salvo el subordinado que taxá las circunstancias agravantes (269H), son fundamentales, en tanto que se aplican sin sujeción a ningún otro; de mera conducta, en tanto que no precisan para su configuración de un resultado material que deba seguirse de la realización de la conducta; de sujeto activo común, en tanto que no precisan de una calidad especial y no puede afirmarse que la ausencia de autorización, facultad u orden judicial a la que aluden sea un calificante; comisivos, en tanto que describen conductas prohibidas; y dolosos, en tanto que precisan de conocimiento y voluntad y, por ende, ninguno admite modalidad culposa. La mayoría contemplan penas de prisión entre 48 y 96 meses y multas de 100 a 1000 SMLMV

Centrémonos en el primer capítulo de la Ley 1273 de 2009 "De los Atentados Contra la Confidencialidad, la Integridad y la Disponibilidad de los Datos y de los Sistemas Informáticos":

- Acceso abusivo a un sistema informático: El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático[7] protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión […] (Ley 1273, 2009, art. 269A).

Se trata de un tipo (i) compuesto de conducta alternativa: tanto acceder total o parcialmente como mantenerse contra la voluntad del sujeto con derecho sobre el sistema consuma la acción típica; (ii) abierto: no delimita con claridad la conducta descrita en él, porque emplea expresiones de relativa vaguedad como, por ejemplo, "por fuera de lo acordado"; (iii) pluriofensivo: por regla general, esta conducta afectará el bien jurídico de la información y los datos y el bien jurídico de la intimidad, consagrado en el Capítulo VII del Código Penal.

Aquí parece que se califica al sujeto cuando se hace referencia a un ingreso "por fuera de lo acordado" o a una estadía renuente en el sistema, pues en estos casos, para que la acción sea

[7] "Por sistema informático se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa" (Ley 1928, 2018, art. 1)

típica, se requeriría que al sujeto activo se le haya conferido permiso para ingresar, pero aquel haya excedido los límites, materiales o temporales, de este.

- Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos[8] allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión […] (op. cit., art. 269B)

Se trata de un tipo (i) compuesto de conducta alternativa: tanto impedir como obstaculizar el funcionamiento o el acceso a lo referido en el tipo consuma la acción típica; (ii) abierto: no delimita con claridad la conducta descrita en él, porque emplea expresiones de relativa vaguedad como, por ejemplo, "acceso normal"; (iii) monofensivo: por regla general, esta conducta afectará únicamente el bien jurídico de la información y los datos.

- Interceptación de datos informáticos. El que, sin orden judicial previa[9] intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático incurrirá en pena de prisión […] (op. cit., art. 269C)

Se trata de un tipo (i) simple: interceptar es la única conducta descrita, solo que recae sobre dos objetos materiales[10], datos informáticos y emisiones electromagnéticas; (ii) cerrado: contiene multiplicidad de elementos normativos, pero fácilmente delimitables; (iii) pluriofensivo: por regla general, esta conducta afectará el bien jurídico de la información y los datos y el bien jurídico de la intimidad, consagrado en el titulo III, capítulo VII del Código Penal.

- Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión […] (op. cit., 269D)

[8] Por "datos informáticos" se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático (Ley 1928, loc. cit,)

[9] El artículo se refiere a la orden que puede emitir el fiscal para, válidamente, interceptar comunicaciones, retener correspondencia o buscar selectivamente en bases de datos (Ley 906, 2004, arts. 233, 235 y 244.)
[10] Objeto materiales la persona o la cosa sobre la cual recae la conducta descrita en el tipo penal

Se trata de un tipo (i) compuesto de conducta alternativa: tanto dañar como borrar, deteriorar, alterar o suprimir lo referido en el tipo consuma la acción típica; (ii) cerrado: contiene multiplicidad de elementos normativos y verbos rectores, pero fácilmente delimitables; (iv) pluriofensivo: por regla general, esta conducta afectará el bien jurídico de la información y los datos y el bien jurídico del patrimonio económico, consagrado en el t
Título VII, Capítulo I, del Código Penal, en el entendido de que la información es susceptible de valoración económica.

- Uso de software malicioso[11]. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión […] (op. cit., art. 269E)

Se trata de un tipo (i) compuesto de conducta alternativa: tanto producir como traficar, adquirir, distribuir, vender, enviar, introducir o exportar software malicioso consuma la acción típica; (ii) cerrado: contiene multiplicidad de elementos normativos y verbos rectores, pero fácilmente delimitable; (iii) monofensivo: por regla general, esta conducta afectará únicamente el bien jurídico de la información y los datos.

- Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes[12], incurrirá en pena de prisión […] (op. cit., art. 269F)

Se trata de un tipo (i) compuesto de conducta alternativa: tanto obtener como compilar, sustraer, ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar o emplear datos personales ajenos consuma la acción típica; (ii) abierto: no delimita con claridad la conducta descrita en él, porque contiene multiplicidad elementos normativos vagos, como "ficheros", "códigos personales" o "medios semejantes"; (iii) pluriofensivo: por regla general,

[11] También se suele usar el termino *malware*. Se trata de programas especialmente diseñados para corromper la estructura del sistema operativo y (o) sustraer información de forma ilegitima.
[12] Es lo que se conoce también como *hacking*.

esta conducta afectará el bien jurídico de la información y los datos y el bien jurídico de la intimidad, consagrado en el Título III, Capítulo VII del Código Penal.

Este tipo, a diferencia de los anteriores, consagra un particular elemento subjetivo, distinto o adicional al dolo[13], según el cual la conducta, para ser típica, debe realizarse con el propósito de obtener provecho. El provecho no debe ser económico y puede ser en favor del autor o de un tercero.

- Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión […].

  En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza[14], siempre que la conducta no constituya delito sancionado con pena más grave

  […] (op. cit. 269G).

Los verbos rectores descritos en el primer párrafo deben ser realizados con objeto ilícito, con finalidad de *pishing*. De no exigirse este elemento subjetivo la conducta carecería de lesividad, como la de aquel estudiante de ingeniería informática que crea su propio sitio web en cumplimiento de una tarea académica.

La conducta descrita en el segundo párrafo, como ilustran Peréz et al. (2010), consiste en que el suplantador, o *phisher*, crea una página y un dominio similar al de la entidad a la cual desea abordar y lo ubica en el espacio de un servidor, o *hosting*, desde donde envía correos *spam* o engañosos. Al no distinguir la página original de la falsa, las personas inocentemente

[13] También llamados elementos subjetivos del injusto, aluden a particulares finalidades, distintas de aquella que es constitutiva de dolo, o a particulares motivos, por los que ha de realizarse la conducta descrita en el tipo
[14] Es lo que se conoce también como *phishing*. Este término proviene de la palabra inglesa *fishing*, que significa pescar, y es utilizado para sugerir el intento de hacer que los usuarios "piquen el anzuelo".

suministran información personal, incluyendo claves bancarias, que el suplantador almacena en una base de datos para luego transferir los activos o el dinero de la víctima a cuentas de terceros partícipes, que luego reclama o distribuye.

Establece la parte final "siempre que la conducta no constituya delito sancionado con pena más grave", adoptándose un criterio subsidiario de aplicación, pues esta especie de conducta puede fácilmente degenerar en delitos como estafa o falsedad personal, marcaria o documental.

Con todo, se trata de un tipo (i) compuesto de conducta alternativa: tanto diseñar como desarrollar, traficar, vender, ejecutar, programar o enviar páginas web con fines ilícitos, o hacer *phishing*, consuman la acción típica ; (ii) abierto: no delimita con claridad la conducta descrita en él, porque tiene un amplísimo ámbito de aplicación, dada la gran cantidad de verbos rectores; (iii) pluriofensivo: por regla general, esta conducta afectará el bien jurídico de la información y los datos, el bien jurídico de la intimidad, consagrado en el Título III, Capítulo VII del Código penal, y el bien jurídico del patrimonio económico, consagrado en el Título VII, Capítulo I, del mismo Estatuto.

De acuerdo con el articulo 269H, las penas imponibles de acuerdo con los artículos descritos se agravarán cuando la conducta se cometa sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros; o cuando se origine o promueva por un funcionario público; o cuando se dé a conocer el contenido de la información en perjuicio de otro; o cuando se realice para obtener provecho para sí o para un tercero; o cuando se actúe con fines terroristas para atentar contra la seguridad o defensa nacional; o cuando se use como instrumento a un tercero de buena fe; o cuando quien incurra en estas conductas sea responsable de la administración, manejo o control de la información.

Repárese, respecto de las situaciones agravantes, en tres cosas:

Los cinco primeros tipos analizados (269A – 269E) no precisan, como requisito de la tipicidad de la conducta, de un elemento subjetivo distinto o adicional al dolo. Pero sí se consagra, en el numeral 5 del 269H, como agravante de ellos, el que la conducta sea realizada en provecho para el autor o un tercero. En el evento del 269F esta agravante sería inaplicable, por vulneración del *non bis in idem*. El evento del 269G es particular porque pese a que ya se consagra un particular elemento subjetivo, la agravante podría aplicarse, porque el fundamento

de los dos elementos subjetivos es distinto: mientras uno habla de objeto o finalidad ilícita, como requisito de la tipicidad, el otro habla de provecho para sí o un tercero, como circunstancia agravante. Aclaremos que la agravante de "fines terroristas" es perfectamente aplicable a todos los tipos, pero el artículo la limita a los eventos en que se persiga una afectación de la defensa o seguridad nacionales.

Ningún tipo analizado individualiza, como requisito de la tipicidad de la conducta, un resultado material que deba seguirse como consecuencia de la realización de la estas. Sin embargo, se consagra, en el numeral 4 del 269H, como agravante de todos ellos, el que la información se revele en perjuicio de otro.

Ningún tipo, excepto por la teoría que planteamos en el 269B, califica el sujeto activo. No obstante, si el sujeto activo está calificado, bien por ser servidor público o bien por tener la administración, manejo o control de la información, la pena a imponer se agravará.

Para finalizar, las agravantes faltantes de consideración son simples: requiere mayor punición la conducta que recaiga sobre ciertos objetos materiales (redes nacionales, sistemas informáticos extranjeros, comunicaciones del sector financiero, etc.); y la conducta que se ejecute usando un instrumento ciego (autoría mediata), o tercero de buena fe.

Prosigamos con el segundo capitulo de la Ley 1273 de 2009 "De los Atentados Informáticos y otras Infracciones". En este capítulo se individualizan conductas que menoscaban no solo la información y los datos, sino también otros intereses jurídicos. El análisis subsiguiente se escinde del anteriormente hecho.

- Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código

Se trata de un tipo (i) autónomo: califica la clásica figura del hurto[15] en atención a su forma de ejecución (ii) simple: describe una única conducta consistente en apoderarse[16] de cosa mueble ajena; (iii) de resultado material: apoderarse es aquello que consuma el delito (iii) de sujeto activo común: no precisa ninguna calidad (iv) abierto: no delimita con claridad la conducta descrita en él, porque contiene multiplicidad elementos normativos; (iv) pluriofensivo: por regla general, esta conducta afectará el bien jurídico de la información y los datos y el bien jurídico del patrimonio económico, consagrado en el Título VII, Capítulo I, del mismo Estatuto; (v) comisivo; (vi) doloso.

Este tipo consagra dos elementos modales: la manipulación de sistemas informáticos y (o) la suplantación de usuarios, con miras a superar medidas de seguridad.

En el proyecto de ley se buscó la eliminación de esta figura, pues según algunos congresistas ya existían tipos que genéricamente recogían la esencia del comportamiento a reprimir; por ejemplo, el hurto calificado por "escalonamiento o llave sustraída o falsa, ganzúa o cualquier otro instrumento similar, o violando o superando seguridades electrónicas u otras semejantes" (Primera ponencia del proyecto de ley 1273, Senado, 2008).

- Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión […] La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Este tipo consagra un particular elemento subjetivo, distinto o adicional al dolo, según el cual la conducta, para ser típica, debe realizarse con el propósito de obtener provecho económico. El provecho puede ser en favor del autor o de un tercero.

---

[15] "El que se apodere de una cosa mueble ajena, con el propósito de obtener provecho para sí o para otro, incurrirá en prisión […]" (Ley 599, 2000, art. 239)

[16] En el apoderamiento el sujeto activo ejecuta un desplazamiento de la cosa a su ámbito de poder, con lo cual destruye de hecho la relación posesoria del sujeto pasivo y establece una nueva de contenido fáctico (Universidad Externado de Colombia, 2011, p. 949)

Este tipo es comúnmente conocido como "estafa electrónica". Esta denominación es oportuna. En la estafa se precisa, para su configuración dogmática, la concurrencia de cuatro elementos: artificio, error, disposición patrimonial y perjuicio; en la transferencia de activos no consentida, igual. La única diferencia es que en el tipo bajo análisis el artificio debe ser informático, electrónico o semejante.

Establece la parte final del primer inciso "siempre que la conducta no constituya delito sancionado con pena más grave", adoptándose un criterio subsidiario de aplicación, pues esta especie de comportamiento puede fácilmente degenerar en delitos como suplantación personal, falsedad documental, estafa u otros. En el segundo inciso se sancionan cuatro conductas consistentes, básicamente, en proveer los medios informáticos para la comisión de la estafa electrónica.

Con todo, se trata de un tipo (i) autónomo: modifica la clásica figura de estafa, sin remitir a ella (ii) compuesto de conducta alternativa: tanto estafar en la modalidad descrita como fabricar, introducir, poseer o facilitar programas destinados a ello consuma la acción típica; (iii) de resultado material "dual": se debe verificar la efectiva transferencia y el perjuicio a un tercero (iii) de sujeto activo común: no precisa ninguna calidad (iv) abierto: no delimita con claridad la conducta descrita en él, porque contiene multiplicidad elementos normativos; (iv) pluriofensivo: por regla general, esta conducta afectará el bien jurídico de la información y los datos y el bien jurídico del patrimonio económico, consagrado en el Título VII, Capítulo I, del mismo Estatuto; (v) comisivo; (vi) doloso.

3. Impacto de la regulación nacional de cara a los delitos informáticos

Vistas las razones de creación de la Ley 1273 de 2009 y los tipos penales que contiene, podemos proceder a evaluar, echando mano de estadísticas oficales, cuál ha sido el impacto de esta y a concluir el trabajo con una corta reflexión.

Lo que se dirá a continuación fue extraído del informe Tendencias de Cibercrimen en Colombia (2019), elaborado por la Policía Nacional.

La dinámica actual del Cibercrimen en Colombia refleja un crecimiento gradual en el número de incidentes cibernéticos reportados a las autoridades del ecosistema de ciberseguridad

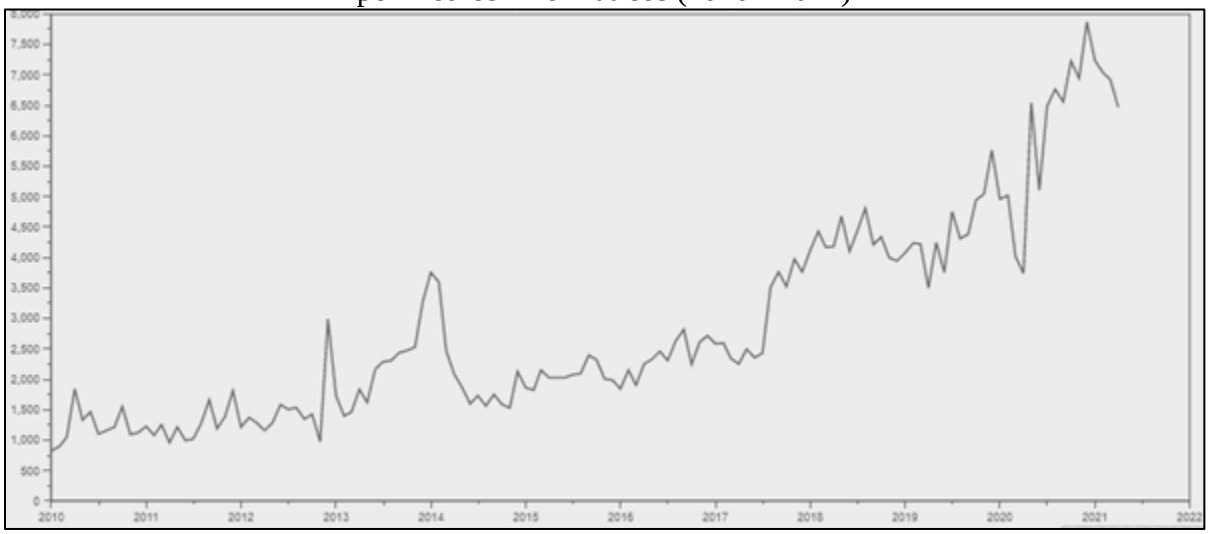
(Policía Nacional, op. cit., pág. 2). A través de los canales de atención a empresas y ciudadanos dispuestos por la Policía Nacional fueron registrados 28.827 casos durante el 2019 (Policía Nacional, loc. cit.). Del total de los casos registrados, 15.948 fueron denunciados como infracciones a la Ley 1273 de 2009 por parte de las víctimas, esta cifra corresponde al 57% del total de casos informados (Policía Nacional, loc. cit.). Respecto al 2018 las denuncias disminuyeron un 5.8 % tras una variación negativa de 983 casos.

El 45% del total de denuncias por ciberdelitos en el país se hace a través de la aplicación A Denunciar. Desde julio de 2017 se han recibido un total 24.711 denuncias por ciberdelitos en esta plataforma virtual (Policía Nacional, op. cit., pág. 4).

12.879 incidentes cibernéticos, es decir, un 43% de los casos reportados en 2019, fueron gestionados sin que se llegara a instaurar una denuncia ante la Fiscalía General de la Nacional (Policía Nacional, loc. cit.).

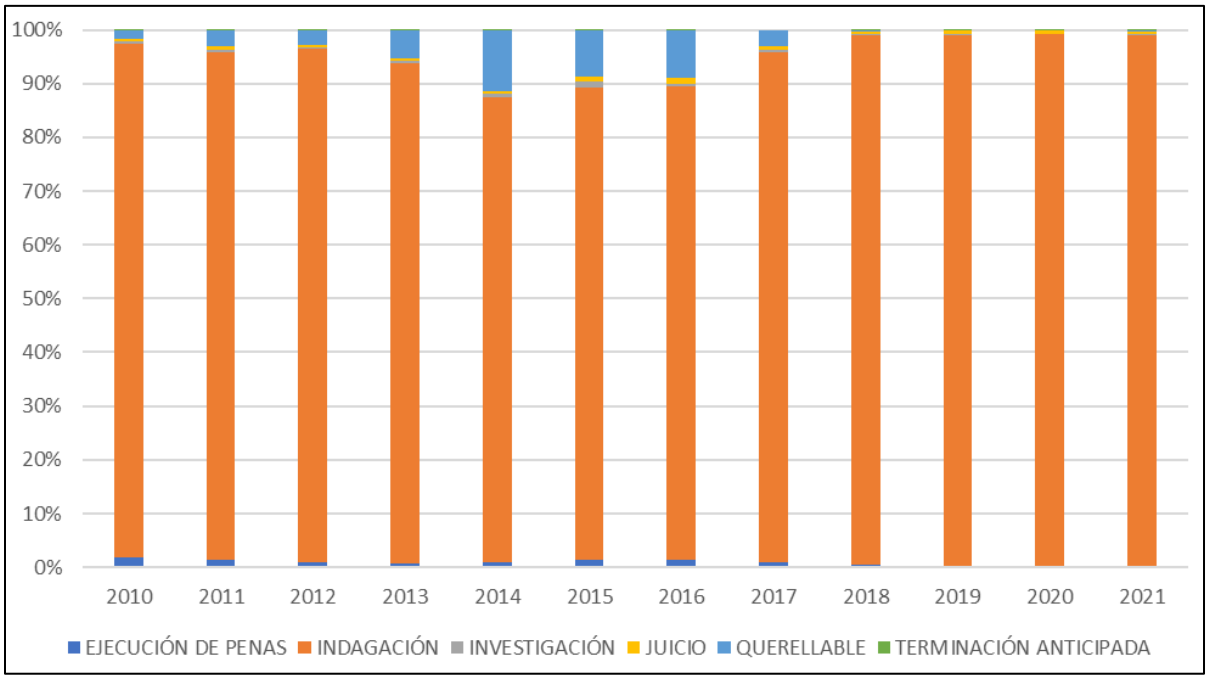
El delito informático más denunciado en Colombia es el Hurto por medios informáticos con un total de 90.893 casos contados desde 2010 a la fecha. Los cibercriminales saben que el dinero está en las cuentas bancarias y por eso buscan comprometer los dispositivos utilizados en la interacción entre usuarios y banca.

Numero de noticias criminales de Hurto
por medios informáticos (2010 –2021)



Fuente: Fiscalía General de la Nación. Ultima actualización: 30 de abril de 2021

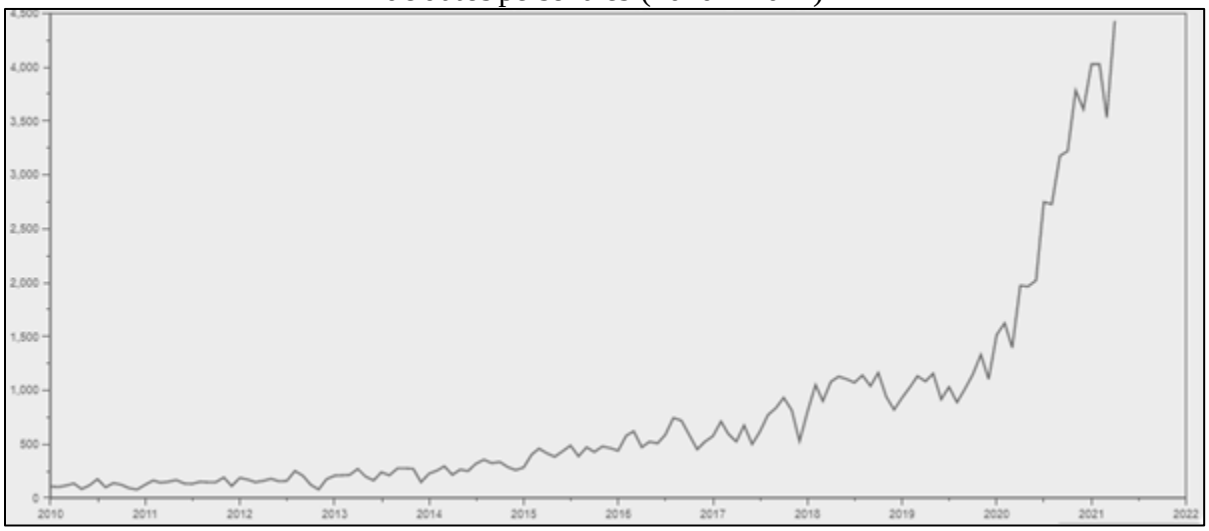
Estadio procesal de las noticias criminales de Hurto por medios informáticos (2010 -2021)



Fuente: Fiscalía General de la Nación. Ultima actualización: 30 de abril de 2021

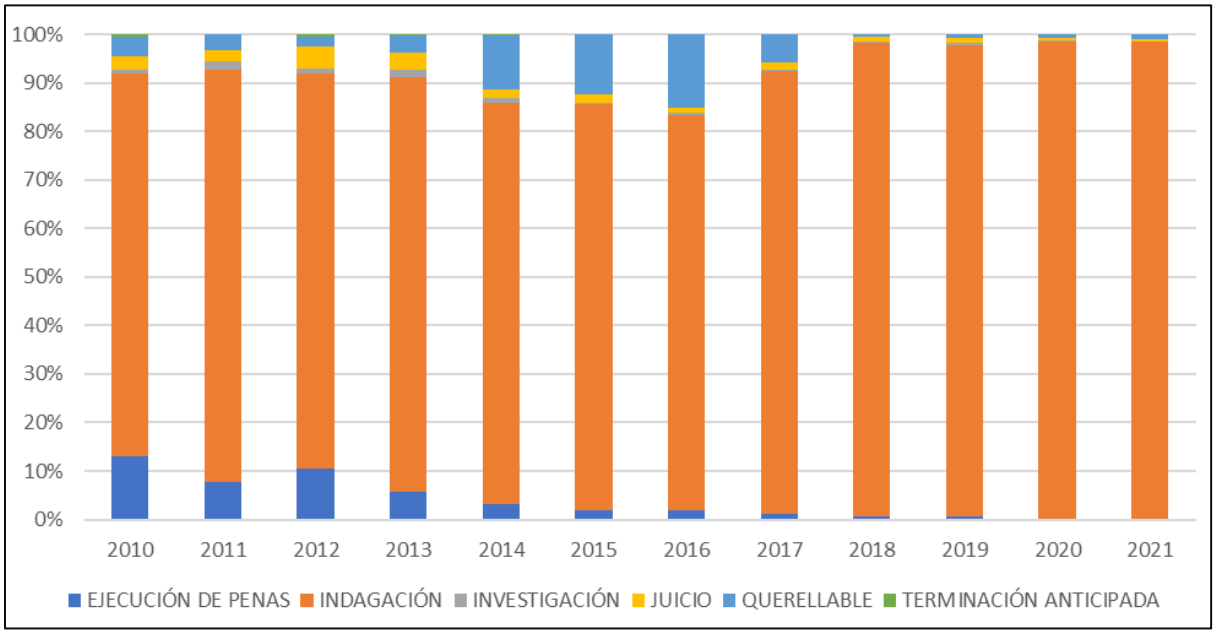
En segundo lugar, se encuentra la Violación de datos personales con 25.735 casos, teniendo un su principal pico en el año 2019. Este dato revela que la segunda amenaza en Colombia para empresas y ciudadanos es el robo de identidades.

Numero de noticias criminales de Violación de datos personales (2010 – 2021)



Fuente: Fiscalía General de la Nación. Ultima actualización: 30 de abril de 2021

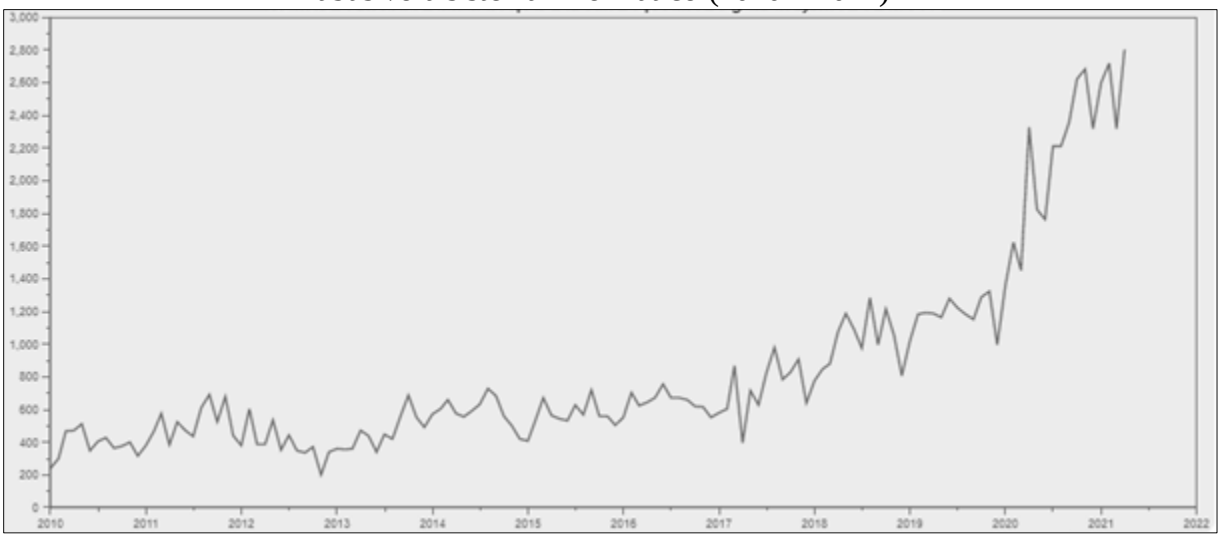
Estadio procesal de las noticias criminales de Violación de datos personales (2010 -2021)



Fuente: Fiscalía General de la Nación. Ultima actualización: 30 de abril de 2021

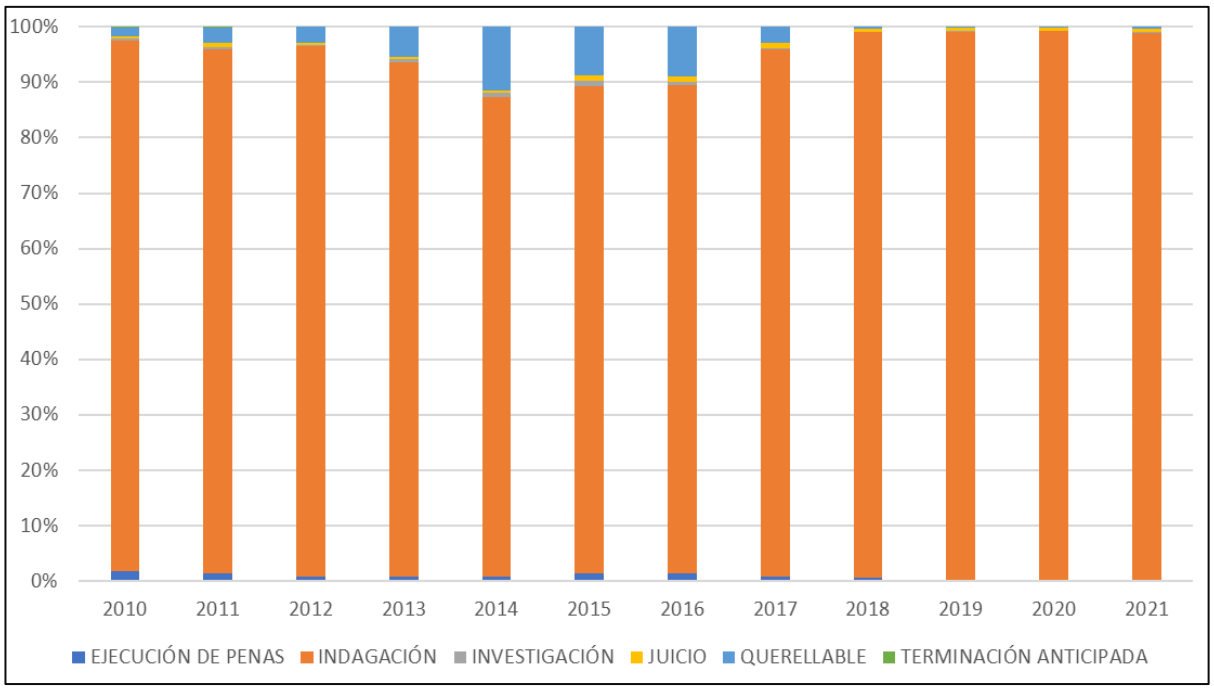
El tercer delito más denunciado es el Acceso abusivo a sistema informático con 21.714 casos, y esto se explica en razón a que, en las fases primarias de los ciberataques, los cibercriminales buscan comprometer los sistemas informáticos logrando ganar el acceso a los mismos. (Policía Nacional, op. cit., pág. 6)

Numero anual de noticias criminales de Acceso abusivo a sistema informático (2010 – 2021)



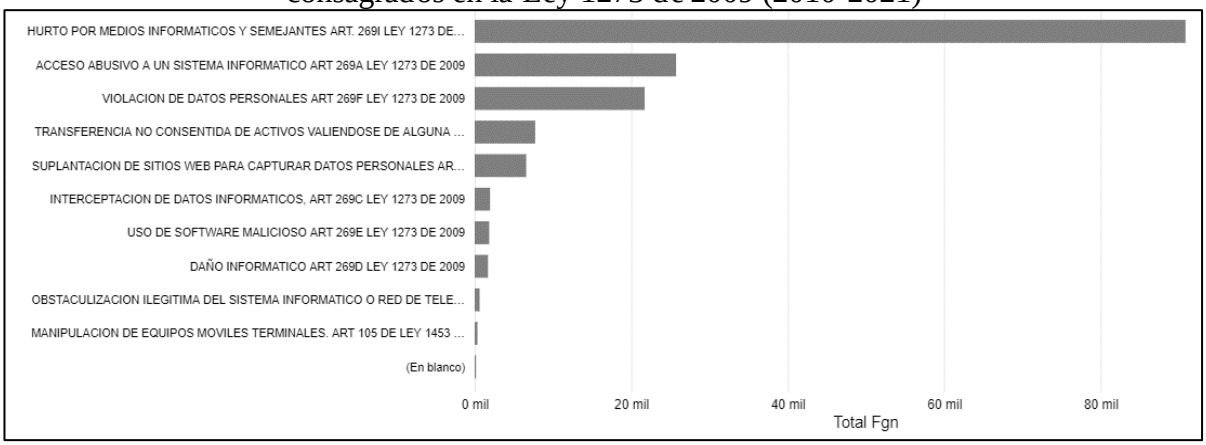
Fuente: Fiscalía General de la Nación. Ultima actualización: 30 de abril de 2021

Estadio procesal de las noticias criminales de Acceso abusivo a sistema informático (2010 -2021)



Fuente: Fiscalía General de la Nación. Ultima actualización: 30 de abril de 2021

Número total de noticias criminales de los delitos consagrados en la Ley 1273 de 2009 (2010-2021)



Fuente: Fiscalía General de la Nación. Ultima actualización: 31 de diciembre de 2020
Elaboro: Subdirección de Gestión Informática en Justicia - Observatorio de Política Criminal.

Siguiendo el citado informe de la Policía Nacional (op. cit., pág. 6), la concentración del fenómeno criminal en 2019 sitúa a Bogotá, Cali, Medellín, Barranquilla y Bucaramanga como las ciudades con mayor afectación por esta problemática con un 55% de los casos registrados. Si bien la cifra obedece a los centros urbanos con mayor densidad poblacional y penetración

de internet en el país, el factor de desarrollo económico influye en los objetivos de los cibercriminales, que enfocan su actuar hacia PYMES, entidades financieras y grandes compañías con asiento en estas ciudades.

4. Conclusiones

En esta monografía se analizó el bien jurídico de la información y de los datos en clave criminológica y político criminal; se ahondó en la clasificación dogmática de los tipos agrupados bajo aquel; y, por último, se evaluó estadísticamente el impacto de esta regulación de delitos informáticos. Después de todo, podemos concluir que la criminalización de estos delitos fue producto del feroz avance de la informática y que los tipos penales que las consagran son, por regla general, básicos, de conducta alternativa, de mera conducta, abiertos, de sujeto activo común, pluriofensivos, comisivos y dolosos. Además, digamos que la decisión adoptada por el Congreso de la República en el año 2009, consistente en criminalizar aquellas conductas que atenten contra la información y los datos, siguió los lineamientos trazados por el Convenio de Budapest del año 2001.

En otras palabras, la determinación de proferir leyes internas en concordancia con el convenio referido, del cual Colombia no era parte, en otras palabras, atendió a la evidente expansión del uso de los sistemas informáticos en el territorio nacional. Así, el sector privado y público, dependientes de estos ciber sistemas, precisaban una protección jurídica integral con miras a preservar datos digitales (secretos industriales y empresariales, finanzas, estrategias de venta, etc.) los cuales, de caer en manos equivocadas, podrían ser usados en detrimento de la honra o patrimonio del afectado (a).

En el trasegar de esta tesis, concretamente, nos adentramos en los motivos de creación de la Ley 1273 de 2009, para luego desentrañar los comportamientos delictivos que esta consagra. Dicha ley constituyó un avance considerable en materia de prevención y represión de ciberdelitos, porque al reconocer la autonomía del bien jurídico penal de la información y de los datos, posibilitó a las victimas la presentación de denuncias por el menoscabo de intereses que antes carecían de protección, por ser todos ellos un mero apéndice, pequeño y desconocido, de otros bienes jurídicos como el de la intimidad. Sin embargo, en el afán de protección se dieron algunos desatinos como lo es la competencia de los jueces para dirimir los delitos

informáticos: en principio, la competencia seria de jueces municipales, pero si nos vamos al precepto general del código de procedimiento penal encontramos que si el delito supera la cuantía de 150 S.M.L.V será de conocimiento de los jueces penales del circuito, por lo cual, en un caso hipotético de un Hurto por medios informáticos que involucre grandes sumas de dinero, puede existir la doble interpretación de quien realmente podrá tener la competencia.

Pese a su regulación, año tras año las denuncias por cibercrímenes aumentan, lo cual refleja que este es un fenómeno en expansión. El dinamismo es una de las principales características de los delitos informáticos pues cada poco tiempo surge un nuevo método para llevar a buen puerto su comisión. Colombia debe caminar paralelamente al desarrollo de este fenómeno, valiéndose para el efecto de personas que comprendan las filigranas del universo virtual. Los fiscales son personajes secundarios en la novela que protagonizan los ciberdelincuentes. Aquellos tienen una posibilidad mínima, prácticamente nula, de dar con estos, si no reconocen sus carencias de conocimiento del particular. A lo que se pretende apuntar es que esta lucha no ha terminado, ni terminará, y que seguirá habiendo criminales impunes, a menos que el derecho penal se alié, se integre con disciplinas que sepan cómo funciona ese fenómeno del cual los especialistas en derecho apenas ven la superficie.

Referencias bibliográficas

1. Baquerizo, J. Z. (1991). *El fenómeno criminal*. Revista jurídica de la Universidad Católica de Santiago de Guayaquil, 1.

2. Becharla-Palacios, Y, Mosquera-Palacios, A., & Ledezma, E. (2020). *Análisis jurídico de la Ley 1273 de 2009 y el surgimiento y expansión del delito de hurto y semejantes por medios informáticos*. Quibdó: Universidad Cooperativa de Colombia.

3. Beling, E. v. (1944). *Esquema del derecho penal*. Buenos Aires.

4. Carrara, F. (1971). *Programa de derecho criminal*. Bogotá D.C.: Temis.

5. Carrasquilla, J. F. (1982). *Derecho penal fundamental*. Bogotá D.C.: Temis.

6. Conde, F. M., & García Arán, M. (2010). *Derecho penal parte general*. Valencia: Tirant lo blanch.

7. Ferri, E. (1933). *Principios de derecho criminal*. Buenos Aires: Depalma.

8. Fiscalía General de la Nación (31 de abril de 2021). *Estadísticas de denuncias por delitos.* [Grafica]. Recuperado de https://www.fiscalia.gov.co/colombia/gestion/estadisticas/delitos/

9. Garofalo, R. (1885). *La criminología*. Madrid: Valleta Ediciones.

10. Gómez, N. (2002). *Escolios a un texto implícito*. Selección. Bogotá D.C.: Villegas Editores.

11. Jescheck, H. H. (1996). *Tratado de derecho penal parte general*. Perú: Instituto Pacífico.

12. Kelsen, H. (1994). *Teoría general de las normas*. México: Trillas.

13. Liszt, F. v. (1889). *Kriminalpolitische Aufgaben. Zeitschrift fir die gesamte Strafre~htswissenschaf.*

14. Liszt, F. v. (1999*). Tratado de derecho penal* (Vol. 1). Madrid: Reus.

15. Mahecha, B. G. (1963). *Curso de derecho penal general*. Bogotá D.C.: Lerner.

16. Manzanera, L. R. (1981). *Criminología*. México D.F: Porrúa.

17. Máynez, E. G. (2002). *Introducción al estudio del derecho*. México D.F: Porrúa.

18. Ojeda-Pérez, J. E., Arias-Flórez, M. E., Rincón-Rodríguez, F., & Daza-Martínez, L. A. (2010). *Delitos informáticos y entorno jurídico vigente en Colombia*. En P. U . Javeriana (Ed.), Cuadernos de contabilidad (págs. 41-66). Bogotá D.C.

19. Olivares, G. Q. (1976). *Represión penal y Estado de Derecho*. Barcelona.

20. Pablos, A. G. (1989). *La aportación de la criminología*. Eguzkilore.

21. Policia Nacional. (2019). *Tendencias del cibercrimen en Colombia*. Bogotá D.C. Obtenido de https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

22. Puig, S. M. (1994). *Antijuridicidad objetiva y antinormatividad en Derecho Penal*. En B. O. estado, & M. d. Justicia (Edits.), Anuario de derecho penal y ciencias penales. España. Obtenido de file:///C:/Users/Usuario/Downloads/Dialnet-AntijuricidadObjetivaYAntinormatividadEnDerechoPen-46453.pdf

23. Reale, M. (1993). *Teoría tridimensional del derecho.* Madrid: Tecnos.

24. Solano, H. R. (2016). *Introducción al estudio del derecho*. Medellín, Colombia: Universidad Pontificia Bolivariana.

25. Solano, H., Duque-Pedroza, A., Díez, M., Arrieta-Burgos, E., Estrada, S., & Monsalve, J. (2019). *Temas de derecho penal parte general. Teoría general del derecho penal*. Medellín: Universidad Pontificia Bolivariana.

26. Universidad Externado de Colombia. (2011). *Lecciones de derecho penal parte especial* (Segunda ed.). Bogotá D.C.: Universidad Externado de Colombia.

27. Valencia, E. T. (2016). *Un viaje a la historia de la informática*. Valencia: Editorial Universidad Politécnica de Valencia. Recuperado el 2021, de http://museo.inf.upv.es/wp-content/uploads/2016/12/Un%20viaje%20a%20la%20historia%20de%20la%20inform%C3%A1tica.pdf

28. Velásquez, F. V. (2020). *Fundamentos del derecho penal*. Bogotá D.C.: Tirant lo Blanch.

29. Zaffaroni, E. R., Alagia, A., & Slokar, A. (2006). *Manual de derecho penal parte general.* Buenos Aires: Edlar.

Referencias normativas

1. Presidencia de la Republica (23 de enero de 1980) Código Penal. [Decreto 100 de 1980]

2. Congreso de Colombia (2007). Exposición de motivos. [Ley 1273 de 2009] GO: 355

3. Congreso de Colombia (2007). Primera ponencia en Cámara. [Ley 1273 de 2009] GO: 528

4. Congreso de Colombia (2007). Segunda ponencia en Cámara. [Ley 1273 de 2009] GO:645

5. Congreso de Colombia (2008). Primera ponencia en Senado. [Ley 1273 de 2009] GO:275

6. Congreso de Colombia. (24 de julio del 2000). Código Penal. [Ley 599 de 2000]. DO: 44.097

7. Congreso de Colombia (1 de septiembre de 2004) Código de Procedimiento Penal [Ley 906 de 2004] DO: 45.658

8. Congreso de Colombia (24 de julio de 2018) Convenio de Budapest [Ley 1928 de 2018] DO: 50.664

9. Congreso de Colombia. (5 de enero del 2009). Ley de delitos informáticos. [Ley 1273 de 2009]. DO: 47.223
10. Corte Constitucional (15 de febrero del 2017) Sentencia C-09 [MP María Victoria Calle Correa]