

ANIVERSARIO EN COLOMBIA DEL NUEVO DELITO DE VIOLACIÓN DE DATOS PERSONALES.

PRIMER AÑO DE VIGENCIA DE LA LEY DE DELITOS INFORMÁTICOS

(Ley 1273 Enero 5 de 2009)

Por Alexander Díaz García

1. Antecedentes históricos

Cumplimos hoy un maravilloso año de triunfo académico, un trabajo arduo de concienciación a la judicatura y a jurisconsultos, con el nuevo tema del delito informático, labor que comenzamos hace más de diez (10) años, con duras y largas jornadas nocturnas de investigación en mi Despacho como Juez de la República en Rovira, logrando que muchas veces se filtrara la luz del nuevo día por entre las rendijas de la ventana que enseña los cerros de la Laguna y Esmeralda, con bastos cultivos de maíz y caña. Logramos finalmente sacar el texto del proyecto que soportó la hoy denominada Ley de Delitos Informáticos (1273 de 2009)

Aún recuerdo como con los trabajos de investigación del proyecto debajo del brazo, golpeé muchas puertas de legisladores locales y nacionales que hicieron caso omiso a la invitación que lo presentaran ante el Congreso de la República; logré finalmente contactar al ex Senador **LUIS HUMBERTO GÓMEZ GALLO**, quien aceptó registrarlo en el Parlamento, labor que lo acompañó el Representante a la Cámara **CARLOS ARTURO PIEDRAHITA CÁRDENAS**, con el que había compartido escenario en una oportunidad en el Auditorio del Palacio de Justicia de Las Alpujarras en Medellín, precisamente disertando sobre delitos informáticos, por dilecta invitación que me hiciera el Dr. Gabriel Roldan, Director de Asuntos Jurídicos y Parlamentarios del Colegio de Jueces y Fiscales de Antioquia.

Los Honorables Congresistas registraron el texto y por técnica legislativa, se acordó que su trámite se haría por Cámara y sería su ponente el Dr. Piedrahita, perteneciente a la Comisión Primera de ese Cuerpo Colegiado, quien lo lideró brillantemente. Trámite que no fue sencillo pues en una de mis intervenciones se suscitó discusión dialéctica con el hoy ex Director del Programa Cuánto Sabe y Cuánto Aprendió Dr. Germán Navas Talero (en el que participé por allá en los años 80's) rechazando rotundamente el proyecto de ley, arguyendo que nuestro

Código Penal no necesitaba de modificaciones e irónicamente afirmaba que lo que pretendíamos era una codificación costumbrista, olvidando los presupuestos acordados por naciones avanzadas en el Convenio del Consejo de Europa sobre cibercrimen, en donde 43 los países la suscribieron, más de 23 lo han ratificado.

En la convención de Budapest, como se le conoce también, se establecen aspectos muy importantes como: medidas a ser tomadas respecto a la legislación sustantiva y disposiciones procesales; medidas relacionadas con la cooperación internacional y asistencia mutua; y normas relacionadas con la firma, ratificación, interpretación y aplicación de la propia convención.

También se contemplan las obligaciones respecto de la colaboración, extradición, intercambio de información y procedimiento relativo a las demandas de colaboración en ausencia de acuerdo internacional. Igualmente, se establecen las obligaciones entre los firmantes en orden a la cooperación en materia de medidas cautelares y asistencia en relación a los poderes de investigación. Es de vital importancia, que a nivel mundial se concrete este acuerdo con la finalidad de lograr controlar, enjuiciar y eliminar el delito informático, que crece día a día adquiriendo novedosas modalidades. Nosotros nos hemos puesto a tono con la comunidad internacional.

Pero los tropiezos no eran sólo en el Congreso, también los teníamos en la Mesa de Trabajo del Ministerio de Relaciones Exteriores, en donde asistí por delegación expresa que me hiciera el Señor Viceministro de Justicia, Dr. Guillermo Reyes, mi Maestro en la especialización de Constitucional y Administrativo. Se intentó también quitarme la vocería, desconozco los motivos, del proyecto en la Cancillería Colombiana, en donde había puesto en consideración de los miembros de la misma el proyecto de ley, a la postre el único que se había presentado; se argüía que no sería de buen recibo en el Congreso puesto que se inclinaban por una norma procesal y no sustantiva como era nuestro trabajo, afirmación que realizaba el delegado del Señor Fiscal General de entonces.

Pero este no fue el único escollo, el Senador Parmenio Cuéllar Bastidas, ex Ministro de Justicia de Colombia, registró ponencia negativa para hundir el trámite logrado hasta este momento en la Cámara, la que por fortuna se superó en la Comisión Conciliadora para finalmente lograrse el cinco (5) de enero de 2009, la sanción presidencial.

Alguien que no puedo olvidar y de la larga lista de participantes en el trámite legislativo, fue el acompañamiento minucioso y dinámico que realizó mi amigo el Dr. Harvey Rincón Ríos, Director de Postgrado de la Universidad Santiago de Cali,

él y esa Alma Mater, creyeron en esta investigación y me patrocinaron mis diferentes intervenciones que tuvimos que realizar fuera y dentro del país, para convencer a la academia y judicatura de la necesidad del proyecto, el que finalmente logramos convencer y sacarlo adelante.

2. Estructura de la Ley

En la investigación, la que realizamos por algo más de diez años, establecemos primero que todo, elevar a bien jurídico tutelado la información y el dato, siendo nuestra legislación una de las pocas amparando la información a tal nivel; se dejaron finalmente siete de los diez artículos que originalmente habíamos sugerido, se excluyeron tipos tan importantes como la **FALSEDAD INFORMÁTICA, ESPIONAJE INFORMÁTICO** y el **SPAM**, le modificaron el epígrafe a la **ESTAFA INFORMÁTICA** por **TRANSFERENCIA NO CONSENTIDA DE ACTIVOS**. Por fortuna no se tocó el que considero uno de los más importantes adelantos legislativos del país, con el derecho penal comparado, **LA VIOLACIÓN DE DATOS PERSONALES**, pues nos tornamos en uno de los pocos países en el mundo de darle una protección penal a los datos personales, pues otras naciones se la dan administrativamente con las Agencias de Protección de Datos Personales en donde existen, Colombia es huérfana con este ente.

La ley la integran, tres artículos en dos capítulos, en el primer Capítulo aparecen los delitos de: **ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO, OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN, INTERCEPTACIÓN DE DATOS INFORMÁTICOS, DAÑO INFORMÁTICO, USO DE SOFTWARE MALICIOSO, VIOLACIÓN DE DATOS PERSONALES, SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS Y CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA.**

En el segundo Capítulo, lo constituyen: **HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES, TRANSFERENCIA NO CONSENTIDA DE ACTIVOS** y termina con el texto de los artículos segundo y tercero, que se refiere a circunstancias de mayor punibilidad y la competencia que no comparto, se radica en cabeza de los Jueces Municipales.

3. El nuevo delito de violación de datos personales

La poca cultura que ha tenido Colombia en la historia sobre el tratamiento de Datos Personales, nos obliga (ya me había referido en anterior trabajo publicado), a pensar que será un proceso largo concienciar a los especialistas judiciales, a los operadores de ficheros que almacenen datos personales, al igual que al público en general, sobre cómo debemos tratar nuestros datos personales y darle la relevancia personal y jurídica que le corresponde

La existencia del artículo 269 F, ha generado y generará muchas (más) implicaciones modificatorias sociales y oficiales; no sólo la consumación ex profeso del delito, sino también para hacer correctivos a costumbres mal sanas que violan los datos personales en el diario vivir de los colombianos.

Esta investigación frenará o por los menos disuadirá a los delincuentes informáticos a no cometer esta clase de infracciones, Vg. Cuando se publica información sensible en redes sociales, cuando se actualiza una obligación prescrita sin el consentimiento del titular¹, en los ficheros de compañías que compra cartera castigada, para mantener ilegal e indefinidamente los registros negativos en las centrales de riesgo. Cuando en los bancos o terceros se apropian de la identidad de una persona sin su consentimiento, para hacerla aparecer como

¹ Corte Constitucional Colombiana. Sentencia T-421/09. Referencia: expediente T-2250851 Acción de tutela instaurada por Abel Mateus contra FENALCO Bogotá. Magistrada Ponente: Dra. MARIA VICTORIA CALLE CORREA Bogotá, D.C., veintiséis (26) de junio de dos mil nueve (2009) En esta sentencia la Corte establece que las obligaciones prescritas no podrán aparecer en las Centrales de Riesgos, como dato negativo. Considero que teniendo en cuenta la Sentencia C-1011 de 2008, con base en criterios de proporcionalidad y razonabilidad rechazó la permanencia indefinida del dato financiero negativo y en consecuencia, declaró la constitucionalidad del artículo 13, que señala las reglas para la Permanencia de la información, bajo el entendido que: *“(...) el término de permanencia de cuatro años también se contará a partir del momento en que se extinga la obligación por cualquier modo”*

La Sala advierte que el dato negativo, no puede permanecer por más tiempo del fijado en la jurisprudencia de este tribunal, esto es, por más de cuatro años contados a partir del momento en el que la obligación se extinga por cualquier modo. Lo contrario, implicaría la vulneración del derecho al Habeas Data del accionante y por tanto, la pertinencia de las acciones judiciales necesarias para amparar el derecho vulnerado. No obstante, observa la Sala que, en el caso estudiado fue acertado la decisión de los jueces de instancia en negar el amparo solicitado por el accionante, debido a que estos carecen de competencia para definir si la obligación se encuentra prescrita, y por tanto, si le asiste derecho al accionante. Así, teniendo en cuenta que la caducidad del dato negativo financiero por extinción de la obligación, depende, para este caso, de la prescripción de la misma, debe el actor acudir a las autoridades competentes para que sea fijada la fecha exacta en la que se dio la prescripción de la obligación contraída con CONFENALCO, para así determinar el momento a partir del cual, de acuerdo con los parámetros fijados por la sentencia C-1011 de 2008, el ciudadano puede solicitar el retiro del dato negativo que reposa a su nombre. Información encontrada en visita realizada en el día de hoy 8 de Diciembre de 2009, a la siguiente url: <http://www.corteconstitucional.gov.co/relatoria/2009/t-421-09.htm>

clientes o deudores de grandes sumas de dinero. Estos son algunos de tantos casos que se conocen con la violación de datos personales.

Igual ocurre cuando las entidades públicas ora sus contratistas para cumplir fines de programas del Estado, capturan información sensible sin advertir que la calidad de la información que entregan los ciudadanos a los encuestadores o representantes de éstos, ha de dársele un tratamiento especial por tratarse de datos personales. Hemos observado que en los formularios o dispositivos electrónicos no aparece información pertinente en donde se concluya un tratamiento especial por la calidad, veracidad, confiabilidad, pertinencia y por consiguiente su prohibición a divulgación o a dársele un fin diferente al originalmente argüido por el empadronador.

Ahora bien, en el ámbito judicial se tendrá que modificar muchas costumbres sobre el manejo de datos personales, ciertamente estamos intentando que se logre, con nuestra demanda de inconstitucionalidad (Expediente D007915) que el Juez de Control de Garantías conozca previamente actos de la Policía Judicial dirigidos por el Delegado del Fiscal, cuando se intenta acceder a ficheros en donde almacenen datos sensibles, derecho especialmente protegido por la norma procesal en su artículo 14², que protege la intimidad.

Para el caso que nos ocupa tenemos el contenido del artículo 237 del Código de Procedimiento Penal, en donde se afirma que se podrá recuperar información dejada al navegar por la Internet u otros medios similares, Vg. Dispositivos de almacenamiento masivo y luego legalizarla ante el Juez Constitucional, lo que a todas luces se vulneran los datos personales pues si bien es cierto que el informático forense no sabe qué clase de contenido encontrará tendrá el fichero por abrir, no descartamos de igual manera que halle información sensible (sus preferencias sexuales, vocación religiosa, vinculación sindical o partidista, origen étnico o datos de salud)

Igual suerte corre, afirmamos en la demanda, con los datos sensibles del imputado que los van a comparar con los resultados de los exámenes invasivos que le han realizado al imputado o indiciado, contemplados en el artículo 245. Nuestra tesis es que se requiere de la anuencia previa del Juez de garantías para acceder a los ficheros clínicos o médicos de éstos para realizar los cotejos científicos pertinentes.

² Código de Procedimiento Penal Colombiano.

Finalmente hemos de afirmar las dificultades que crea la vigencia de la Ley 1266 del 31 de Diciembre de 2008, la estatutaria de Hábeas Data. Dificultades que deberá superar la Fiscalía General de la Nación, pues los delegados del Señor Fiscal, son los que están haciendo uso de dicha información. Veamos cuál:

Dice textualmente el artículo 308 del Código de Procedimiento Penal, que el Juez de Control de Garantías, a petición del Fiscal General de la Nación o de sus Delegados, decretará la medida de aseguramiento cuando de los elementos materiales probatorios y evidencia física recogidos y asegurados o de la información obtenidos legalmente, se puede inferir razonablemente que el imputado puede ser autor o participe de la conducta delictiva que se investiga siempre y cuando se cumpla alguno de los siguientes requisitos:

“1. Que la medida de aseguramiento se muestre como necesaria para evitar que el imputado obstruya el debido ejercicio de la justicia

2. Que el imputado constituye un peligro para la seguridad de la sociedad o de la víctima (Subrayas nuestras)

3. Que resulte probable que el imputado no comparecerá al proceso o que no cumplirá la sentencia.”

El Delegado en la mayoría de las ocasiones soporta su súplica en el numeral dos, que es desarrollado a su vez por el artículo 310 ibídem, modificado igualmente por el artículo 24 de la Ley 1142 de 2007, que en su tenor literal dice:

“Peligro para la comunidad. Para estimar si la libertad del imputado resulta peligrosa para la seguridad de la comunidad, será suficiente la gravedad y modalidad de la conducta punible. Sin embargo de acuerdo con el caso, el Juez podrá valorar adicionalmente alguna de las siguientes circunstancias: (Subrayas nuestras)

1.

2.

3. *El hecho de estar acusado, o de encontrarse sujeto a alguna medida de aseguramiento, o de estar disfrutando un mecanismo sustitutivo de la pena privativa de la libertad, por delito doloso o preterintencional*

4. *La existencia de sentencias condenatorias vigentes por delitos doloso o preterintencional.”* (Subrayas nuestras)

El Delegado para fundamentar que el imputado requiere medida de aseguramiento intramural (privativa de la libertad) presenta a las partes y al Estrado, un

documento en donde se registran anotaciones y antecedentes, expedido por el DAS, en donde la institución de seguridad advierte que: *“Sin comprobación dactiloscópica e ignorando si se trata de la misma persona, figura (n) siguientes anotación (es) y antecedente (es):.....”*

Documento que si no tiene soporte de alguna otra naturaleza, como la verificación decadáctilar del imputado con ficheros de altísima confianza (Vg. Los propios de la Fiscalía), no puede servir para materializar las pretensiones procesales del Delegado. Recordemos que así lo exige el artículo 128 de la obra citada, que fuera igualmente modificado por el artículo 11 de la Ley 1142 de 2007, en donde señala que la Fiscalía General de la Nación estará obligada a verificar la correcta identificación o individualización del imputado, a fin de prevenir errores judiciales.

Pasaremos a analizar por qué el documento del DAS en estudio, no sirve en las condiciones que usualmente lo están haciendo los Delegados del Señor Fiscal General de Colombia:

El artículo 2º de la Ley de Hábeas Data, reza que la ley se aplicará sin perjuicio de normas especiales que disponen la confidencialidad o reserva de ciertos datos o información registrada en banco de datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público. Dicho enunciado nos permite colegir fácilmente que los ficheros del DAS, se cobijarán por esta ley.

Ahora bien, la ley en estudio en su artículo 4º que aparece bajo el epígrafe de Principio de la Administración de Datos, dice que el desarrollo, interpretación y aplicación de la presente ley, se tendrán en cuenta, de manera armónica e integral, los principios que a continuación se establecen:

“a) Principio de veracidad o calidad de los registros o datos. La información contenida en los Bancos de Datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error;...”. (Subrayas nuestras)

Concatenando el contenido de estos artículos con la afirmación de los oficios de anotaciones y antecedentes del DAS de marras, estos no pueden prestar ningún merito (al menos hasta cuando no se modifique lo anotado) para el soporte de una medida de aseguramiento, con base en el argumento de que es un peligro para la comunidad. Es más al final de estos documentos (los del DAS) advierten en letra menuda que: *“La anterior información deber ser tratada con la reserva legal correspondiente y su utilización es de absoluta responsabilidad de la autoridad solicitante, razón por la cual el manejo indebido, causará las sanciones previstas*

en la ley (art. 4 Decreto 3738 de 2003) (Subrayas nuestras) Esto es que, pese al error que pudiera existir en la información, el DAS se exonera y será de exclusiva responsabilidad del usuario, esto es, el Delegado del Señor Fiscal General.

Conocemos de casos en donde aparece en el prontuario una orden de captura con más de seis meses³ (Art. 298 ejusdem), pero no aparece ningún otro reporte que nos indique que efectivamente si se ha capturado al imputado, o se le precluyó la investigación. Igual suerte corren los datos de una imputación, una medida de aseguramiento o una captura, sin más datos posteriores. Esta información es incompleta, no está actualizada y puede ser que no sea veraz porque puede tratarse de un sujeto completamente diferente al que se encuentra en ese momento en la Sala de Audiencias.

3. Efectos de la ley y sus estadísticas

Lograda la sanción Presidencial hoy hace un año precisamente, por parte del Dr. Álvaro Uribe Vélez, Presidente de Colombia, comenzamos otra ardua tarea, la concienciación de la academia y de la judicatura sobre el tema, para superar la gran crítica que se recibe sobre el tema, la falta de capacitación del personal que tienen que ver con los delitos informáticos. Así estamos evitando comentarios como el de Guillermo Santos Calderón⁴: *“Otra duda que me surge es sobre el conocimiento que deben tener los jueces que van a enfrentar estos casos. Los delitos del mundo de la informática tienen tantas facetas y tantos matices, que requieren de algún grado de profundidad en los términos y las técnicas que se deben manejar para poder analizar con veracidad y en forma estricta si se cometió algún delito”*.

Efectivamente como formador de ICITAP (International Criminal Investigative Training Assistance Program) del Departamento de Justicia de los Estados Unidos, y acompañado de los Ings. John Jairo Echeverri Aristizábal y Edwin Alexander Cifuentes, miembros de la Unidad de Delitos Informáticos del CTI de la

³ Artículo 299 del Código de Procedimiento Penal, ordena taxativamente que se deberá comunicar que la orden de captura ha perdido la vigencia, para descargarlas de los ficheros de cada organismo, indicando el motivo de tal determinación. Mandato que no ocurre con riguroso cumplimiento.

⁴Comentario que realiza el periodista del periódico EL TIEMPO, al referirse sobre la vigencia de la nueva ley de Delitos Informáticos. Visita que se realizó el cinco de enero de 2010 al siguiente site: http://www.eltiempo.com/opinion/columnistas/guillermosantoscaldern/ARTICULO-WEB-PLANTILLA_NOTA_INTERIOR-4722899.html

Fiscalía General de la Nación, el Delegado del Señor Fiscal General de la Nación Dr. Jairo Sánchez y nuestro Coordinador del Grupo de Delitos Informáticos, Dr. Fernando Cañón Beltrán, hemos logrado visitar en un año de trabajo incansable, unas veinte (20) ciudades del país, entre otras Valledupar, Montería, Riohacha, Cartagena, Santa Marta, Barranquilla, Medellín, Cúcuta, Bucaramanga, Paipa, Yopal, Leticia, Florencia, Cali, Pereira, Armenia, Manizales, Bogotá, Villavicencio e Ibagué, y formar más de seiscientos (600) funcionarios judiciales, entre Delegados del Fiscal General, Ingenieros y Técnicos de Sistemas del CTI, de Contralorías Departamentales y de la Policía Nacional.

Según aporte que me realiza la Unidad de Delitos Informáticos del CTI, tenemos el siguiente cuadro acerca del número de casos que se están llevando en este momento o se han tramitado para su investigación, a saber:

DESCRIPCION DE LA ACTUACION	Vienen	Asignadas	Total Practicadas	Canceladas	Pendientes	Practicadas Efectivas
ACCESO ABUSIVO A UN SISTEMA INFORMATICO	0	2	0	0	2	0
VIOLACION DE DATOS PERSONALES	0	18	18	0	0	18
HURTO POR MEDIOS INFORMATICOS y SEMEJANTES.	2	50	20	2	30	17

Observamos cómo el Hurto por Medios Informáticos y Semejantes (Art. 269 I) es el tipo de mayor incidencia delincriminal con cincuenta (50) investigaciones, sobre dieciocho (18) que tiene la Violación de Datos Personales (Art. 269 F) y dos (2) de Acceso Abusivo a un Sistema Informático (Art. 269 A) Esta ley ha generado una mayor ocupación en la Unidad de Delitos Informáticos del CTI, de la Fiscalía General de la Nación, pues ha implicado a conocer nuevos procedimientos, diferentes a los que se usaban antiguamente con la evidencia material, pues al tratarse de evidencia digital o lógica, ello ha generado una mejor preparación por parte del personal técnico, nacional e internacionalmente y adecuarse a los estándares de ese grado para el manejo de esta clase de prueba procesal, el documento electrónico, a continuación detallamos los procedimientos forenses que se realizan en tratándose de delitos informáticos ora delitos clásicos consumados a través de medios electrónicos.

CONSOLIDADO GENERAL DE ACTUACIONES								
DELITOS	Vienen	Asignadas	Total Practicadas	Canceladas	Pendientes	Practicadas Efectivas		
ANALISIS DE DOCUMENTOS			0	2	1	0	1	0
ANALISIS A SISTEMA DE INFORMACION O SISTEMA TELEMATICOS			0	9	3	3	3	1
ANALISIS DE SOFTWARE			0	3	3	0	0	3
ANALISIS FINANCIERO			0	1	1	0	0	1
ANALISIS Y/O RECUPERACION DE INFORMACION DE MEDIOS DE ALMACENAMIENTO DIGITAL			46	116	88	4	70	77
BUSQUEDA EN BASES DE DATOS			0	60	42	0	18	35
DUPLICACION DE INFORMACION OBTENIDA EN MEDIO DE ALMACENAMIENTO DIGITAL			0	1	1	0	0	1
ANALISIS INFORMatico			30	65	45	6	44	39
RASTREO DIRECCION IP			31	80	61	4	46	34

Ahora bien analizaremos las estadísticas de la Policía Nacional, gracias al aporte que nos hiciera el Mayor Fredy Bautista y la It. Claudia Pestaña, funcionarios de la Policía Nacional División DIJIN Delitos Informáticos, me ha clasificado el comportamiento punible informático por Departamentos y encontramos que el Hurto por Medios Informáticos y Semejantes es el tipo más consumado en el país con doscientas veinte (220) denuncias, siendo la ciudad de Cali Valle como de mayor incidencia con sesenta y cinco (65) investigaciones, le sigue muy lejos el Acceso Abusivo a un Sistema Informático con siete (7) y la región de Colombia con una mayor vulneración es el Magdalena con cuatro (4) investigaciones. La siguiente gráfica los ilustrará mejor y ustedes sacarán sus propias conclusiones.

**POLICÍA NACIONAL
DIRECCIÓN DE INVESTIGACIÓN CRIMINAL**

DELITOS INFORMATICOS REGISTRADOS EN EL PAIS AÑO 2009

UNIDAD POLICIAL	ARTÍCULO 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	ARTÍCULO 269G. SUPlantación DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	ARTÍCULO 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS	TOTAL
CALDAS				6		6
CESAR				1		1
MAGDALENA	4			12		16
MAGDALENA MEDIO				5		5
META				1		1
NARIÑO				1		1
RISARALDA	1					1
VALLE	1			4		5
M. BUCARAMANGA				1		1
M. CALI	1	1		65	6	73
M. BARRANQUILLA				11		11
M. BOGOTÁ				25	1	26
M. CÚCUTA				45		45
M. MEDELLÍN				6		6
URABÁ			1	6		7
BOYACÁ				31		31
TOTAL	7	1	1	220	7	236

INFORMACION EXTRAIDA DEL ISTEMA SIEDCO EL DÍA 05 DE ENERO DE 2010, 15:00 HORAS, SUJETA A VARIACIÓN POR DENUNCIAS QUE INGRESAN POR SIDENCO AL SISTEMA PENAL ORAL ACUSATORIO.

Finalmente no podemos olvidar que el delito de publicación de datos personales en redes sociales, no es exactamente una injuria o calumnia y es por ello que dicha columna correspondiente a este delito, se han sumado al tipo clásico correspondiendo al delito informático.

5. Conclusión

La vigencia de esta ley, protegiendo el bien jurídico tutelado de la INFORMACIÓN y el DATO, ha posesionado el país en el contexto jurídico que estaba en mora de ubicarse. Por fortuna se superaron las dificultades legislativas y la mayoría de los miembros del Congreso entendieron que les correspondía a ellos, tipificar estas conductas que lamentablemente se están masificando en su consumación. A la par del desarrollo tecnológico informático, la delincuencia encuentra formas innovadoras para la realización de fraudes y otros delitos que, con frecuencia, van más rápido que los códigos penales. De una o de otra forma, la comisión de algún delito informático afecta a un mayor número de ciudadanos. Frente a un fenómeno en alza, se impone la necesidad de prevención y protección, que son deber de todos: Estado, empresas, organizaciones, ciudadanía.

Siguiendo con los propósitos de ICITAP, lograremos con un gran esfuerzo y con la participación masiva por parte de los Delegados, la Policía Judicial de la Fiscalía General de la Nación y demás cuerpos de seguridad del país, capacitar con los más altos estándares para contrarrestar el delito informático. Evitaremos de esta manera tipificaciones erradas, como se hacia antiguamente con la publicación indebida e ilegal de datos personales en redes sociales, conexión o acceso a redes sin autorización, uso de software malicioso etc. Con esta nueva ley se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Alexander Díaz García. Abogado de la Universidad Católica de Colombia. Especialista en: Ciencias Penales y Criminológicas de la Universidad Externado de Colombia; Ciencias Constitucionales y Administrativas de la Universidad Católica de Colombia y en Nuevas Tecnologías y Protección de Datos de la Escuela de Gobierno y Políticas Públicas de Madrid, adscrita a la Instituto Nacional de Administración Pública de España. Autor de la primera Acción de Tutela Electrónica, protegiendo los Derechos Fundamentales de Hábeas Data y la Intimidad Virtual, por abuso de spam. Autor del Proyecto de Ley de Delitos Informáticos, hoy Ley 1273 de 2009. Instructor del Departamento de Justicia de los Estados Unidos en el programa ICITAP (International Criminal Investigative Training Assistance Program) en el Módulo de Delitos Informáticos, capacitando a Fiscales e Ingenieros de Sistemas del CTI. Autor de la Acción de Inconstitucionalidad ante la Corte Constitucional, en contra de los artículos 237 y 245 del Código de Procedimiento Penal, por violación de datos personales. Actualmente Juez Segundo de Control de Garantías de Rovira Tolima Colombia

Contactos alediaganet@gmail.com