"LA PROBLEMÁTICA EXISTENTE EN EL NUEVO SISTEMA INTEGRADOR DE HISTORIAS CLÍNICAS ELECTRÓNICAS DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES VINCULADA AL DERECHO A LA PRIVACIDAD DE LOS PACIENTES Y LA PROTECCIÓN DE SUS DATOS PERSONALES"

DIRECTOR: Dr. Sandro Abraldes

ALUMNA: Candela Belén Fernández Rasillo

NRO. ID DE REGISTRO: 000-15-9168

PROGRAMA: Especialización en Derecho Penal

UNIVERSIDAD: Universidad de Belgrano

TUTOR: Dr. Gustavo Aboso

FECHA DE PRESENTACIÓN: 18 de junio de 2020

INDICE

INTRODUCCIÓN AL PLAN DE TRABAJO

1.- Área temática**:** derecho constitucional, mala praxis médica y criminalidad informática.

2.- Objetivo general**:** demostrar que el acceso indebido al Sistema Integrador de Historias Clínicas Electrónicas (el cual contiene el Registro de Historias Clínicas Electrónicas de la Ciudad Autónoma de Buenos Aires) ya sea para la incorporación, la modificación y/o la divulgación de la información de los pacientes allí registrados- configura un delito de acceso ilegitimo, especialmente si el autor resulta ser un agente confidente, es decir, cuando el ingreso lo efectúa el propio médico o el programador del sistema vulnerándolo desde adentro.

3.- Planteo del problema**:** el ingreso de manera ilegítima al Sistema Integrador de Historias Clínicas Electrónicas y al Registro de Historias Clínicas Electrónicas de la Ciudad Autónoma de Buenos Aires (ley nro. 5669 de la Ciudad Autónoma de Buenos Aires) vulnera tanto el derecho a la privacidad de las personas (art. 19 de la Constitución Nacional), los derechos del paciente en su relación con los profesionales e instituciones de salud (ley nro. 26.529), como así también el derecho a la protección de los datos personales (leyes nro. 25.326 y nro. 1845 de la Ciudad Autónoma de Buenos Aires).

Buscaré con el presente trabajo argumentar los motivos por los cuales creo que mediante el ingreso online -debido o indebido- al sistema de mención, no es posible garantizar de manera fehaciente el resguardo de los datos personales y sensibles de los pacientes que se encuentran registrados.

En tal sentido expondré los motivos que me llevan a sostener que la manipulación de terceros respecto de la información allí suministrada, ya sea ingresando correctamente a aquel desde aparatos tecnológicos de dichas instituciones, o mediante la comisión de algún tipo de delito informático (157 bis del Código Penal de la Nación), podría permitir que dichos datos se utilicen maliciosamente o con algún provecho personal y/o económico, configurándose así el delito previsto en el art. 117 bis del Código Penal de la Nación (modificado por el art. 32 de la ley 25.326).

Puntualmente, haré alusión a ello teniendo en cuenta que se trata de una gran cantidad de individuos los que poseen ingreso a la plataforma referida, tratándose tanto de profesionales o auxiliares de la salud en establecimientos asistenciales, públicos, privados, de la seguridad social (en situaciones de emergencia médica o en consultorios particulares), como del personal que integra la Comisión de Seguimiento de las Historias Clínicas Electrónicas, los cuales son representantes de diversos establecimientos sanitarios -art. 30, inciso 9 de la ley nro. 5669 de la Ciudad Autónoma de Buenos Aires-.

PRIMERA PARTE**:** *El marco teórico y jurídico del derecho fundamental en lo que atañe a la protección de datos personales y de carácter sensible.*

a) El derecho a la privacidad de las personas (art. 19 de la Constitución Nacional y art. 11, incisos 2 y 3 de la Convención Americana sobre Derechos Humanos)

Tal como puede leerse en la primera parte del apartado señalado por la Constitución Nacional *"Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados".* Esto nos habla de un principio primordial: el derecho a la intimidad, respecto del cual ya tiene dicho la doctrina que *"(...)es aquél que tiene una persona de disponer de una esfera o espacio privado sin que el Estado o los particulares se entrometan. Se protege así un espacio de autonomía individual integrado por sentimientos, creencias religiosas, familia, hábitos y costumbres, etc. El derecho a la privacidad es la posibilidad de realizar acciones privadas".*[1]

Así, muchas veces este derecho se presenta como un medio para reforzar la importancia de otros -tanto en la red como por fuera de ella-, incluyendo aquellos que protegen a la igualdad y a la no discriminación, o los que salvaguardan la libertad de expresión y de reunión.

Otro de los reconocidos doctrinarios que analizó en profundidad el mentado artículo fue Quiroga Lavié quien sostuvo que *"La afectación de la intimidad no sólo se produce invadiendo el ámbito real del individuo afectado, sino también a través de la propagación de datos que deforman la realidad".*[2]

El más alto tribunal se ha expedido en varias oportunidades respecto de este derecho fundamental y constitucional, afirmando que *"El derecho a la privacidad comprende no sólo a la esfera doméstica y al círculo familiar y de amistad, sino a otros aspectos de la personalidad espiritual o física de las personas tales como la integridad corporal o la imagen, nadie puede inmiscuirse en la vida privada de una persona ni violar áreas de su actividad no destinada a ser difundidas, sin su consentimiento o el de los familiares autorizados para ello, y sólo por ley podrá justificarse la intromisión siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución de un crimen".*[3]

---

[1] Andrea M. Orihuela. Constitución Nacional Comentada. Sexta Edición. Editorial Estudio. Año 2012. Pág. 64/65.

[2] Humberto Quiroga Lavié. Constitución de la Nación Argentina Comentada. Segunda edición actualizada. Editorial Zavalia. Año 1997. Pág. 116.

[3] CSJN, fallos 316:703, "Gutheim v. Alemán", 15/3/1993.

Dichas bases se asentaron con fuerza y claridad en el fallo Ponzetti de Balbín[4] luego de que la revista *"Gente y Actualidad"* publicara en su tapa una foto del Dr. Balbín en la sala de terapia intensiva de una clínica en un estado agonizante.

Al respecto la Corte adujo que el derecho a la libertad de expresión (que incluye también el dar y recibir información) no es absoluto ni resulta condición suficiente para lesionar la intimidad de una persona (ya que si entran en colisión ambos valores la jurisprudencia reconoció que prevalecerá este último), como es el caso bajo estudio, donde el lesionado, pese a ser una persona pública, debe gozar de cierta esfera íntima.

Agregó que el derecho a la privacidad -al tener rasgo constitucional– protege acciones, hechos o datos que están reservados al propio individuo y cuya divulgación por los extraños significa un peligro para su intimidad. Ello comprende no sólo la esfera doméstica, sino otros aspectos de la personalidad (por ejemplo, la integridad corporal o la imagen) y nadie puede inmiscuirse en la vida de los demás ni violar áreas de su actividad que no estén destinadas a ser difundidas.

Finalmente, expresó que la Convención Americana sobre Derechos Humanos en su art. 11, protege el respeto a la honra y el reconocimiento de la dignidad de cada ser humano, en su vida privada, la de su familia, su domicilio o su correspondencia, protegiéndolo de la injerencia y de los ataques ajenos.

b) El derecho a la protección de los datos personales (leyes nro. 25.326 y nro. 1845 de la Ciudad Autónoma de Buenos Aires)

Ambas normas son prácticamente idénticas en lo que respecta al tratamiento que le dan al resguardo de la información de los sujetos. La principal diferencia radica en el ámbito de aplicación, ya que una tiene alcance en la esfera de la Ciudad Autónoma de Buenos Aires, mientras que la otra debe aplicarse a nivel nacional.

En los primeros artículos definieron ciertos conceptos utilizados comúnmente para hacer alusión a los datos personales, tales como: "*el responsable"* (persona física o de existencia ideal, pública o privada, que sea titular de un archivo, registro, base o banco de datos)*, " el titular"* (persona física o de existencia ideal con domicilio legal, delegaciones o sucursales en el país -o en la Ciudad Autónoma de Buenos Aires- cuyos datos sean objeto de tratamiento) y "*el usuario"* (toda persona, pública o privada, que realice a su arbitrio un tratamiento de aquellos, ya sea en archivos, registros, bancos de datos propios o a través de una conexión con los mismos).

En cuanto a la forma de ser recabados, especificaron que el titular de ellos tendrá que ser anoticiado, debiendo saber cuál será el fin de su recolección, de qué tipo de archivo se tratará, a quién estará destinado, las consecuencias de proporcionarlos (y de

[4] CSJN, "Ponzetti de Balbín Indalia v. Editorial Atlántida S.A", fallos 306-1892, 11/12/1984.

su negativa a hacerlo) o de la inexactitud de ellos, como así también del derecho que tendrá para acceder, rectificarlos o suprimirlos.

Constituyeron un apartado especial para hablar de los datos sensibles, con el fin de aclarar que nadie estará obligado a aportarlos. Sin embargo, una vez que ya se cuente con ellos, podrán ser utilizados sin autorización del titular, únicamente cuando medien razones de interés general autorizados por ley o cuando se manipulen con fines estadísticos/científicos, pero en este último caso, no deberá ser posible identificar a sus propietarios.

Puntualizaron también que, quiénes intervengan en cualquier fase del tratamiento de esta información, estarán obligados al secreto profesional, situación que subsistirá aún después de finalizada su relación con el titular del archivo de esos datos.

Asimismo, agregaron que todo el contenido tendrá que ser claro, estar exento de codificaciones y, en caso de que resulte necesario por su complejidad, deberá acompañarse la respectiva explicación, en un lenguaje accesible al conocimiento medio de la población.

Frente al incumplimiento de todo lo expuesto, dieron lugar a ciertas sanciones penales, reprimidas en los arts. 117 bis y 157 bis del Código Penal de la Nación, figuras que procederé a desarrollar en los siguientes apartados.

Finalmente, ambas leyes le dedicaron diversos artículos a la acción constitucionalmente protegida que poseen todos los individuos para proteger sus datos personales: "*el habeas data"* (art. 43 de la Constitución Nacional), utilizado ya sea para tomar conocimiento de ellos, exigir su rectificación, su supresión, su confidencialidad o su actualización. Esta procederá respecto de los responsables y los usuarios de bancos de datos públicos y/o privados que provean los informes cuestionados. Dicha acción se encuentra por fuera de los límites del derecho penal y es la justicia civil la encargada de resolverla en tal sentido, mediante un juicio sumarísimo.

Se trata principalmente del derecho que asiste a toda persona identificada o identificable a solicitar judicialmente la exhibición de los registros públicos o privados (en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud) y a requerir la rectificación, la supresión de los inexactos, obsoletos o que impliquen cierta discriminación.

Ya se expresó la doctrina al respecto diciendo que *"Diversos bienes jurídicos están involucrados en el habeas data; así, el honor, la imagen, la identidad, la dignidad, la vida privada, la libertad de información, etc.; sin embargo, es de destacar que el que más intensamente se ve comprometido es "la intimidad personal", no tanto en su dimensión negativa, es decir, como rechazo o exclusión de terceros del ámbito de la propia vida privada sino en su dimensión positiva, esto es como afirmación de la propia libertad y dignidad de la persona, en el sentido de revalorizar el derecho del individuo a resolver*

sus cuestiones y tomar decisiones al margen de la influencia de terceros, fundamentalmente en lo que refiere al ejercicio de su libertad en el ámbito de la informática, lo que actualmente se denomina libertad informática o derecho a la autodeterminación informativa".[5]

A su vez se señaló que *"Se intenta canalizar tal protección a través de un concepto abarcativo de diversas circunstancias que engloban el marco de la intimidad de las personas; es decir, de un cúmulo de datos referidos a su íntima personalidad y desarrollo individual. Así, se entiende que dentro de ese universo se encuentra todo lo referido a la identidad, reconociéndose el derecho a la verdad y al control de los datos, que corresponde tanto a las personas físicas cuanto jurídicas, por parte de los sujetos cuya información es objeto de archivos. También, el derecho a la autodeterminación informativa".*[6]

Por lo tanto, según ellos *"(…) la protección de datos personales contiene en sí misma la esencia de un derecho genérico, con contenido específico, que se manifiesta en tres dimensiones: el derecho a conocer, el derecho a acceder y el derecho a rectificar. De esta manera se observa que el hábeas data intenta abordar la problemática de la privacidad, discriminación e información, que conlleva la defensa de la dignidad personal".*[7]

La idea de preservar los datos guarda relación directa con los derechos de tercera generación, consolidados constitucionalmente a fines del siglo pasado. Así, la garantía del habeas data acompaña, sin lugar a duda, al creciente impacto que provocó la informática en las esferas de la intimidad y en la privacidad de las personas.

c) El bien jurídico protegido: la intimidad

La función de la privacidad es, principal y fundamentalmente, ayudar a establecer ciertas fronteras para limitar quién tiene acceso a nuestro cuerpo, lugares y objetos, así como a nuestras comunicaciones e información personal.

Existen ciertas profesiones, como ser el derecho o la medicina, donde de los propios códigos de ética utilizados se cuenta con la figura del *"secreto profesional",* que pone el foco en la preservación de la intimidad de los clientes o los pacientes.

La protección de los derechos fundamentales, y en especial de la intimidad, se vio afectada de una manera particular durante los últimos años, a raíz de la expansión de

---

[5] Carlos A. Chiara Díaz. Código Penal y Normas Complementarias. Comentado, Concordado y Anotado. Arts. 54 al 139 bis. Tomo III. Editorial Jurídica Nova Tesis. Pág. 673.

[6] David Baigún, Eugenio Raúl Zaffaroni y Marco Antonio Terragni. Código Penal y Normas Complementarias. Análisis Doctrinal y jurisprudencial. 5. Artículos 134/161. Parte Especial. Editorial Hammurabi, Buenos Aires. Año 2008. Pág. 813.

[7] David Baigún, Eugenio Raúl Zaffaroni y Marco Antonio Terragni. Código Penal y Normas Complementarias. Análisis Doctrinal y jurisprudencial. 5. Artículos 134/161. Parte Especial. Editorial Hammurabi, Buenos Aires. Año 2008. Pág. 813.

la Internet en todos los sectores de la vida cotidiana, lo cual provocó un desafío para la aplicación de las leyes. Si bien sus principios resultan directamente aplicables, se constató la necesidad de efectuar ciertas precisiones.

En general, hoy por hoy se trata de una tecnología con una capacidad de tratamiento de datos inimaginable para el simple usuario; ya que la mayoría se llevan a cabo de manera invisible, circunstancia que dificulta el control por parte de su titular.

Como tiene dicho el máximo tribunal "*en la era de las computadoras el derecho a la intimidad ya no puede reducirse a excluir a los terceros de la zona de reserva, sino que se traduce en la facultad del sujeto de controlar la información personal existente en estos archivos o bancos de datos".*[8]

Así, cabe destacar que existen numerosos casos donde esto no fue respetado. Un claro ejemplo podría ser el fallo *"Clementi, Edgar Omar y otro vs. Embajada de Rusia y otros s/ Cumplimiento de convenio de honorarios"*, en el cual dos abogados denunciaron a la Embajada de la Federación Rusa luego de su incumplimiento con un convenio de honorarios, suscripto por el entonces embajador de dicha sede, en representación de una misión diplomática, a modo de reconocimiento y en compensación por las tareas profesionales que los actores habrían realizado *"en defensa de los intereses de aquella misión".*

En el marco de ese antecedente, la Corte Suprema de Justicia de la Nación determinó que *"el accionar de los letrados, no solamente violó el principio de la defensa en juicio, sino también los derechos a la privacidad e intimidad de los clientes, garantías que, derivadas del art. 19 de la Constitución Nacional, se cristalizan en normas como la del art. 244 del Código Penal Procesal de la Nación y el art. 156 del Código Penal de la Nación".*[9]

En otra oportunidad, se expidió al respecto aludiendo *"Es por ello que se ha subrayado el carácter transformador de Internet, como medio que permite que miles de millones de personas en todo el mundo expresen sus opiniones, a la vez que incrementa significativamente su capacidad de acceder a la información y fomenta el pluralismo y la divulgación de información (conf. "Declaración Conjunta sobre Libertad de Expresión e Internet", citada ut supra, del 1° de junio del 2011). El acceso a Internet, debido a su naturaleza multidireccional e interactiva, su velocidad y alcance global a un relativo bajo costo y sus principios de diseño descentralizado y abierto, posee un potencial inédito para la realización efectiva del derecho a buscar, recibir y difundir información en su*

[8] CSJN, "Dirección Gral. Impositiva v. Colegio de Abogados de la Cap. Fed.", JA 1996-II-295; LL 1996-B-35; fallos 317:71; 13/02/1996.

[9] CSJN, "Clementi, Edgar Omar y otro vs. Embajada de Rusia y otros s/ Cumplimiento de convenio de honorarios", fallos 330:1804, 17/04/2007.

doble dimensión, individual y colectiva (Comisión Interamericana de Derechos Humanos, "Libertad de Expresión e Internet", citado anteriormente, párrafo 36)".[10]

De igual manera, en otro legajo, el Procurador General señaló que *"(…)Lenkner (Schönke/Schröder, Strafgesetzbuch Kommentar, Múnich, 1991, p.1484) afirma que si el obligado a la confidencialidad obtuvo el conocimiento del hecho porque el autor es su paciente o mandante, sólo existe una autorización para revelar el secreto en casos de altísima peligrosidad para el futuro, y ello tampoco procede si el autor se dirigió al abogado (asunción de la defensa) o al médico (por ejemplo, para el tratamiento de una anomalía de los impulsos) a causa de ese hecho",* concordando así con lo aludido en los párrafos anteriores.[11]

d) Lex artis

Es el conjunto de prácticas médicas aceptadas, por la general, como las adecuadas para tratar a los enfermos. Por definición, resultan ser cambiantes según el progreso técnico de la medicina y las peculiaridades personales de cada paciente. Están constituidas por los principios científicos de la práctica médica para una especialidad determinada o un procedimiento específico.

Se integran con la literatura magistral empleada en las instituciones de educación superior para la formación del personal de la salud y con las publicaciones que demuestren mérito científico y validez estadística. También dependen de los criterios que fije, en su caso, la autoridad sanitaria superior, sugiera la farmacopea autorizada o emitan las comisiones de investigación científico-médica.

Para que la intervención profesional sea legítima debe, además de perseguir el fin de curar y ser la indicada, ejecutarse conforme a las reglas del arte médico. Algunas de ellas están escritas y son las leyes públicas que orientan el ejercicio de la profesión, o constituyen normas dictadas por los colegios profesionales. Sin embargo, la mayoría no poseen forma de ley y están dictadas según la experiencia, pese a lo cual son aceptadas e indican cómo debe actuarse frente a diversas situaciones.

Las obligaciones del médico empiezan a generarse cuando este asume efectivamente sus funciones, ya que desde ese instante se coloca en una posición de protección respecto del paciente, es decir, pasa a adquirir una posición de garante como dueño absoluto del proceso de curación y, en consecuencia, como centro decisorio del mismo.

Será el encargado de formular el juicio de diagnosis, teniendo en cuenta la nosología (rama de la medicina cuyo objetivo es describir, explicar, diferenciar y

[10] CSJN, R. 522. XLIX, "Rodríguez María Belén c/ Google Inc. s/ daños y perjuicios", 28/10/2014.

[11] CSJN, "Baldivieso Cesar Alejandro", causa 4733, B. 436, L. XL, 08/12/2010.

clasificar la amplia variedad de enfermedades y procesos patológicos existentes, entendiéndose éstos últimos como entidades clínico-semiológicas, generalmente independientes e identificables según criterios idóneos) y la nosografía (descripción de la enfermedad), así como las múltiples variantes que presentan las situaciones individuales.

Un diagnóstico adecuado permite conocer anticipadamente la evolución probable de la enfermedad y cuál podrá ser la consecuencia del tratamiento terapéutico que se resuelva adoptar.

e) Los datos de carácter sensible o especialmente protegidos. Su definición y su regulación en el ámbito médico. Diferenciación con los datos de carácter personal y con los datos biométricos.

Los **datos personales sensibles** son aquellos que se relacionan con el nivel más íntimo de cada persona. Su divulgación puede ser la causa de que dicho sujeto sufra algún tipo de discriminación o de generarle un riesgo severo. Se trata de aquella información que revela características muy propias de cada ser humano, como pueden ser, por ejemplo, las opiniones políticas, las creencias filosóficas y/o morales, el origen étnico o racial, el estado de salud, las creencias religiosas, la preferencia sexual, la pertenencia a ciertos sindicatos, etc.

La definición de **datos personales**, en cambio, hace alusión a todas aquellas características generales asociadas a un individuo que lo hace identificable del resto o lo hace pertenecer a cierto grupo específico, como, por ejemplo: el nombre, el sexo, la nacionalidad, la edad, el lugar de nacimiento, la raza, la filiación, el domicilio, el teléfono, etc.

Resta decir que **los datos biométricos** son aquellos rasgos físicos, biológicos o de comportamiento de una persona, que lo identifican como único del resto de la población. Generalmente son usados en ciertos sistemas de seguridad informática en los que se miden como parte del proceso de autentificación del sujeto. Podrían enumerarse algunos puntuales como ser las huellas dactilares, la geometría de la mano, el análisis del iris y/o de la retina, los rasgos faciales, el patrón de la voz, la firma manuscrita, el análisis gestual y/o el de ADN, etc.

En el ámbito local y particularmente en lo que atañe al campo de la medicina, tal como lo establece en su art. 4, inciso 27 la ley nro. 5669 de la Ciudad Autónoma de Buenos Aires, en la actualidad se cuenta con un "*Sistema de Información de Historias Clínicas Electrónicas*", el cual es implementado y administrado por cada establecimiento de salud para capturar, manejar e intercambiar la información estructurada e integrada

de las historias clínicas electrónicas en su poder, la cuales contienen los datos sensibles de cada paciente.

En lo que atañe al ámbito internacional, el Tribunal Europeo de Derechos Humanos argumentó en sus dictámenes que la memorización de los datos relativos a la vida privada de una persona constituye una injerencia en el sentido del art. 8 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales, independientemente de que luego estos sean utilizados o no.

Aclaró que, para determinar si los datos conservados hacen entrar (o no) en juego algún aspecto de la vida privada de las personas deberá puntualizarse el contexto en el que fueron obtenidos y conservados, su naturaleza, la forma en la que fueron tratados y el posible efecto del tratamiento.

Para ello explicó que, para estar justificadas, las injerencias han de poseer tres requisitos obligatorios: una previsión legal, una finalidad legítima y una necesidad que justifique su recolección en una sociedad democrática.

En dicho contexto, el tribunal de Estrasburgo confirmó que en dicha Ciudad será una injerencia por parte del estado de derecho y una violación a la norma mencionada, la mera conservación de datos: **a)** relativos a la vida privada, tales como los que contengan datos sensibles, por ejemplo aquellos relativos a la salud, **b)** cuyo tratamiento automatizado va más allá de una identificación neutra, aunque no sean considerados relativos a la vida personal por sí mismos, **c)** que, debido al carácter sistemático o permanente del registro y por su uso en conjunción con demás datos personales, sean susceptibles de hacer entrar en juego el derecho al respeto de la vida privada, pese a que sean públicos.[12]

SEGUNDA PARTE: *La historia clínica, su origen y evolución.*

a) Concepto

La historia clínica es la relación ordenada y detallada de todos los datos y conocimientos –anteriores, personales, familiares y actuales- relativos a un enfermo, que sirve de base para el juicio acabado de una enfermedad.

La ley de Salud Pública nro. 26.529 (modificada por la ley nro. 26.742), hizo alusión al concepto de *"Información sanitaria"* y la definió en el art. 3 como aquella que, de manera clara, suficiente y adecuada a la capacidad de comprensión del paciente, informa sobre su estado de salud, los estudios y los tratamientos que fueran acordes realizarle, su previsible evolución, los riesgos que conlleva, las complicaciones y las posibles secuelas de estos.

[12] TEDH, causa 30562/04 y 60566/04, "S. Y Marper c/ Reino Unido", 04/12/2008.

De igual forma, en el apartado siguiente especificó que dichos datos únicamente podrán ser brindados a terceras personas con una autorización del paciente.

A su vez, en el art. 12, al hacer alusión a la historia clínica la detalló como un documento obligatorio, cronológico, foliado y completo en el que consta toda la actuación médica realizada sobre una persona.

Destacó su carácter inviolable y puntualizó que los establecimientos asistenciales –públicos o privados- y los profesionales de salud, tienen a su cargo su guarda y custodia, asumiendo el carácter de depositarios con relación a ella, debiendo instrumentar los medios y los recursos necesarios para evitar su acceso a personas no autorizadas.

b) Los elementos constitutivos

Obligatoriedad: esta característica surge de lo establecido en el art. 40 –incisos l y m- del decreto reglamentario de la ley de ejercicio de la medicina, que se refiere al compromiso asumido por los directores de los establecimientos asistenciales de adoptar los recaudos necesarios para que se confeccionen las historias clínicas, se conserven, se archiven y no se vulnere el secreto profesional.

Tal circunstancia aplica con igual carga para los centros médicos, las prepagas, los institutos médicos, las clínicas, las maternidades, los hospitales privados, las obras sociales y los sanatorios.

Contenido: quedó establecido en la práctica profesional que una historia clínica debe registrar: el número adjudicado en la institución en la que se ingrese, los datos del paciente, del familiar o de la persona a consultar en los casos que resulte necesario, los antecedentes hereditarios, familiares y personales anteriores a su dolencia (lo cual recibe el nombre de anamnesis), las fechas de ingreso y egreso del lugar, el estado clínico al momento de su arribo, la evolución diaria y los tratamientos llevados a cabo, las consultas con los especialistas, los partes quirúrgicos o de otro tipo, los exámenes complementarios, el consentimiento informado si fuese necesario, las indicaciones dispuestas por el personal a cargo de su cuidado y la epicrisis.

Confección y redacción: debe ser redactada por el médico de manera personal, ordenada y legible, evitando así el uso de abreviaturas. Cada hoja debe estar debidamente foliada e identificada con el nombre del paciente y el número respectivo de legajo.

Firma: cada actualización que se realice en ella debe ser firmada y aclarada.

Plazo de conservación: en el orden nacional rige la resolución nro. 648/96 de la ex Secretaría de Salud Pública según la cual deben conservarse por el término de quince (15) años.

En la Ciudad Autónoma de Buenos Aires se establece un plazo idéntico en los hospitales de su jurisdicción, tal como estipula el decreto nro. 4182 del año 1985.

c) El consentimiento informado del paciente

Tal como lo definió en el art. 5 la ley de Salud Pública nro. 26.529 (modificada por la ley nro. 26.742), se entiende por consentimiento informado a la declaración de voluntad suficiente, efectuada por el paciente o por sus representantes legales (en los casos que resulte necesario), emitida luego de recibir, por parte del especialista interviniente, la información clara, precisa y adecuada relacionada con su estado de salud, el procedimiento propuesto para su mejoría –con la especificación de los objetivos perseguidos a tal fin-, los beneficios esperados del mismo, los riesgos, las molestias y los efectos adversos previsibles, la especificación de ciertos tratamientos alternativos, la comparación de sus riesgos, beneficios y perjuicios en relación al primeramente propuesto y las consecuencias de la no realización de cualquiera de ellos.

La ley de mención permitió que tal circunstancia pueda realizarse de manera verbal, salvo en ciertos casos particulares donde sí o sí debe hacerse por escrito. Estos últimos son: la internación, la intervención quirúrgica, los procedimientos diagnósticos y los terapéuticos invasivos, ya que conllevan ciertos riesgos.

De igual forma, estipuló que las únicas excepciones a la anuencia del paciente serán cuando exista un grave peligro para la salud pública o una situación de emergencia, con grave peligro para la salud o la vida del paciente y este no pueda darlo por sí o por medio de sus representantes.

El médico no puede actuar sin anuencia de la persona a la que va a atender, ya que en la relación entre ambos deberá prevalecer, como es natural, los derechos del enfermo. Es este último quien puede decidir aceptar o rechazar el tratamiento luego de que el profesional lo interiorice del mismo.

Esta voluntad superior solamente cederá en el instante en que, transpuesto el umbral del consentimiento y luego de ser suficientemente informado, empieza la actuación técnica. Es a partir de allí donde el paciente no podrá interferir en lo que el médico técnicamente decida, ya que es donde sus obligaciones comienzan a regir.

d) ***Los derechos del paciente en su relación con los profesionales y las instituciones de salud***

Según lo dispuesto en el art, 4, inciso c de la ley nro. 153 de la Ciudad Autónoma de Buenos Aires (Ley Básica de Salud) todas las personas tienen el derecho a que se respete su intimidad, su privacidad y la confidencialidad de la información relacionada con su proceso salud-enfermedad.

Así, tal como se reguló en el art. 2 de la ley nro. 26.529 de Salud Pública, modificada por la ley nro. 26.742 (y su decreto reglamentario nro. 1089/2012), los derechos del paciente resultan fundamentales en su relación con los profesionales de la salud, los agentes del seguro de salud y/o cualquier otro efector del que se trate.

Quedan comprendidos los siguientes:

Asistencia: todos los pacientes, principalmente los niños, niñas y adolescentes, tienen el derecho de ser socorridos por los profesionales, sin distinción ni menoscabo alguno, pese a sus creencias religiosas y/o políticas, sus ideas, su condición socioeconómica, su raza, su sexo, su orientación sexual o cualquier otra condición personal.

La única excepción para eximirse de este deber será cuando se hubiera hecho cargo efectivamente del tratamiento otro experto competente.

Trato digno y respetuoso: cada paciente tiene el derecho a que se respeten sus convicciones personales y morales, principalmente aquellas vinculadas con sus condiciones socioculturales, de género, de pudor y de su intimidad, sea cual fuera el padecimiento que posea, circunstancia que se deberá hacer extensiva a los familiares y/o acompañantes.

Intimidad: toda actividad que resulte tendiente a obtener, clasificar, utilizar, administrar, trasmitir y custodiar información/ documentación clínica del paciente, debe asegurar el estricto respeto por la dignidad humana y la autonomía de la voluntad, así como el debido resguardo de su intimidad y la confidencialidad de sus datos sensibles.

Confidencialidad: cada persona que tenga acceso o elabore la documentación que obre en poder de la clínica respecto de un paciente, deberá tener la debida reserva de la misma, salvo expresa disposición en contrario, que emane de una autoridad judicial competente o por medio de una autorización del propio paciente.

Autonomía de la voluntad: el paciente adulto, los niños, las niñas y los adolescentes (éstos últimos tres grupos podrán intervenir en los términos de la ley nro. 26.061) tienen el derecho de aceptar o de rechazar determinadas terapias, procedimientos (tanto médicos como biológicos) con o sin expresión de causa, como así también a revocar una manifestación de voluntad previamente manifiesta.

Información sanitaria: los pacientes deben recibir la información vinculada a su salud que les sea necesaria, pero también están en todo su derecho de decidir no conocerla.

Interconsulta médica: todas las personas tienen derecho a solicitar una copia por escrito de su historia clínica, con el objeto de poder solicitar una segunda opinión sobre el diagnóstico, el pronóstico o el tratamiento relacionado con su salud.

e) La historia clínica digital: su finalidad, las ventajas y los riesgos que la misma conlleva

Tal como lo definió la ley nro. 5669 de la Ciudad Autónoma de Buenos Aires, en el art. 4, inciso 14 y en el art. 9, la historia clínica electrónica es el documento digital, obligatorio, con marca temporal, individualizada y completa, en el que constan todas las actuaciones de asistencia a la salud.

Su registro unificado, personal y multimedia se encuentra contenido en una base de datos administrado mediante programas de computación y refrendado con la firma digital del profesional tratante.

Su almacenamiento, actualización y uso se efectúan en estrictas condiciones de seguridad, integridad, autenticidad, confiabilidad, exactitud, inteligibilidad, conservación, disponibilidad y acceso.

La nombrada es equivalente a la historia clínica registrada en soporte papel, en los términos de la ley nro. 26.529, modificada por la ley nro. 26.742 y su implementación es progresiva, no implicando la derogación de las disposiciones vigentes en materias de historias y registros clínicos compatibles con el soporte informático.

El paciente tiene, durante todo momento, el derecho de conocer la totalidad de los datos allí consignados, conforme lo dispone la ley nro. 25.326 y la ley nro. 1845 de Protección de Datos Personales, como así también tiene la posibilidad de realizar un seguimiento de los accesos efectuados en su historial (art. 18 de la ley nro. 5669 de la Ciudad Autónoma de Buenos Aires).

Esto encuentra sustento en el art. 13 de la ley de Salud Pública que autorizó la confección de una historia clínica en un soporte magnético, siempre y cuando se arbitren los medios necesarios para asegurar la preservación, la autenticidad, la inalterabilidad, la perdurabilidad y la recuperabilidad de los datos allí contenidos en tiempo y forma.

A tal fin, el legislador propuso en el marco de dicha norma el uso de accesos restringidos con claves de identificación, medios no regrabables de almacenamiento, control de modificación de campos o cualquier otra técnica idónea para asegurar su resguardo.

f) El marco normativo del registro de las historias clínicas electrónicas de la Ciudad Autónoma de Buenos Aires y la posterior creación del Sistema Integrador de estas

De la ley nro. 153 de la Ciudad Autónoma de Buenos Aires (Ley Básica de Salud), se desprendió en el art. 12, inciso t, que una de las tantas obligaciones del sistema de salud es lograr el desarrollo de un método de información básica y uniforme para todos los subsectores, incluyendo, a tal fin, el establecimiento progresivo de la historia clínica única.

A su vez, en los incisos p y q del art. 14, se repitió nuevamente tal circunstancia, al proponer que se instituya la historia clínica única para todos los efectores y que se desarrolle un sistema que permita un inmediato acceso a las mismas y a la situación de cobertura de las personas que demanden servicios, garantizando la confidencialidad de los datos y la no discriminación.

Con el objeto de implementar todo ello, la ley nro. 5669 de la Legislatura de la Ciudad Autónoma de Buenos Aires, sancionada con fecha 27 de octubre del año 2016, estableció la existencia del Sistema Integrador de Historias Clínicas Electrónicas (SIHCE) para todos los habitantes que reciban atención médica en esta ciudad, creando a tal fin, la *"Base de Datos Única"* (conjunto organizado de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso) que facilitará el almacenamiento y la gestión de los datos sanitarios, desde el nacimiento hasta el fallecimiento de cada individuo, previamente contenidos en las historias clínicas electrónicas.

Se trató de un repositorio con toda la información sanitaria de los pacientes contenida en las historias clínicas electrónicas, disponible para su consulta mediante redes electrónicas de información de uso público.

Según lo instaurado en el art. 22 de la mencionada ley, los establecimientos de salud que presten el servicio en esta localidad, deben garantizar (bajo la responsabilidad administrativa, civil o penal) la confidencialidad de la identidad de los pacientes, así como la integridad, disponibilidad, confiabilidad, trazabilidad, y no repudio de la información sanitaria, de conformidad con un sistema de gestión de seguridad de la información que debe evitar el uso ilícito o ilegítimo que pueda lesionar los intereses o los derechos del titular de los datos.

En los arts. 27 y 28 de la misma ley surgió con claridad que *"El Registro de Historias Clínicas Electrónicas"* tiene como objetivo principal dictar las normas que sean necesarias para establecer estándares tecnológicos con relación a los datos confeccionados en dichas historias clínicas electrónicas, como así también para las funciones y las características de este.

Agregó que deberá posibilitar los medios para que, luego de su ingreso, se pueda solicitar turnos en línea para la atención en el subsistema público de salud de esta ciudad, desde cualquier dispositivo conectado a internet y que permita, a su vez, requerir prescripciones médicas (en aquellos pacientes que fueron atendidos y observados en forma física y deban consumir fármacos a lo largo del tiempo).

g) Los principios generales de actuación aplicados al tratamiento de los datos personales de la salud según la ley nro. 5669 de la Ciudad Autónoma de Buenos Aires

Accesibilidad: es la posibilidad de ingresar a la información contenida en las historias clínicas electrónicas. La norma enumeró ciertos niveles de acceso: **1)** el de consulta; **2)** el de consulta/ actualización; **3)** el de consulta/ actualización/ modificación de la información, debiendo todos ellos contar con los mecanismos de seguridad pertinentes para verificar la autenticidad de los usuarios (validación de la identidad mediante medios idóneos, que permita identificar de forma unívoca a cada uno de los profesionales que lo utilice).

Disponibilidad: los datos en cuestión deben poder verse en todo momento y desde cualquier establecimiento asistencial público y/o privado con sede en esta ciudad.

Privacidad: la totalidad de la información allí inserta es considerada como un dato personal, confidencial y sensible, por lo que el paciente siempre tendrá el derecho a conocerla.

Portabilidad: posibilidad para el paciente, su representante o sus derechohabientes de obtener una copia de aquella, ya sea mediante un soporte electrónico o en papel.

Seguridad: hace alusión a la preservación de la confidencialidad, la integridad y la disponibilidad de los datos, además de otras propiedades como la autenticidad, la responsabilidad, el no repudio y la fiabilidad.

Inviolabilidad: la información inserta no puede, bajo ningún punto de vista, ser adulterada.

Confidencialidad: los datos deben ser tratados con absoluta reserva y no estarán disponibles para los restantes individuos, entidades ni procesos, salvo autorización del paciente, su representante, el derechohabiente o por disposición judicial.

Veracidad y autoría: todo lo allí inserto debe ser actual y real respecto del diagnóstico, el tratamiento y su posterior evolución.

Durabilidad: el hecho de que el documento y las firmas sean digitales las protege de un posible deterioro.

Integridad: los datos insertos deben ser completos e inalterados.

Temporalidad: la información suministrada tiene que corresponderse con la secuencia cronológica de lo sucedido.

Interoperabilidad y estándares: se trata de la interacción de los establecimientos asociados con objetivos comunes, como por ejemplo lograr obtener beneficios mutuos.

Finalidad: su principal objetivo es que la asistencia sanitaria y los datos contenidos en la misma no se utilicen con otros fines distintos a los detallados anteriormente.

Oportunidad: busca que el registro que efectué el profesional sea registrado de manera simultánea a la atención médica brindada por aquel o inmediatamente después.

***TERCERA PARTE**: Incidencias de las nuevas tecnologías en el ámbito sanitario.*

a) La seguridad y la confidencialidad en torno a la historia clínica digital y al sistema que la resguarda

A partir de lo postulado en el art. 4, incisos 26 y 29 de la ley nro. 5669 de la Ciudad Autónoma de Buenos Aires, apareció la figura del *"Sistema de Gestión de la Seguridad de la Información",* la cual hace referencia a una técnica global que -basada en el análisis de riesgos- establece, implementa, opera, monitorea, revisa, mantiene y mejora la seguridad de la información con la que se trabaja.

A su vez, comprende una estructura de organización, una planificación de actividades y ciertas políticas, responsabilidades, procedimientos, procesos y recursos.

Cabe destacar en ella la existencia de una cualidad imprescindible, como ser la trazabilidad que permite que todas las acciones realizadas sobre la información y/o el sistema de tratamiento de esta, sean asociadas de modo inequívoco a un individuo puntual o a una entidad específica, dejando un inevitable rastro del respectivo acceso.

Dicha ley concluyó que la autoridad de aplicación del sistema detallado será el Ministerio de Salud de la Ciudad Autónoma de Buenos Aires o el organismo que en el futuro lo reemplace o sustituya. Así, se encuentra entre sus funciones principales, la creación de una Comisión de seguimiento de las historias clínicas electrónicas, conformada por representantes de establecimientos sanitarios, del Ministerio de mención, de la Dirección General de Gestión Digital dependiente del Ministerio de Modernización, Innovación y Tecnología de la Ciudad Autónoma de Buenos Aires, de la Comisión de Salud de la Legislatura Porteña y por cualquier otro actor que sea considerado relevante.

b) La protección de los datos personales y el delito previsto en el artículo 157 bis del Código Penal de la Nación. El resguardo de la intimidad y la figurada regulada en el art. 117 bis del Código Penal de la Nación (modificado por el art. 32 de la ley nro. 25.326)

La ley nro. 25.326 de Protección de Datos Personales incorporó al Código Penal de la Nación dos disposiciones sin precedentes en el derecho argentino: la del art. 157 bis, introducida en el capítulo III (Violación de secretos) del título V (Delitos contra la libertad) y la del art. 117 bis.

Esta circunstancia obedeció principalmente a la necesidad de actualizar la ley penal a los cambios que se dieron en el ámbito informático. Con el avance de la tecnología, su posibilidad de tratar y de almacenar gran cantidad de datos personales, surgió la necesidad de amparar penalmente la violación de la reserva de ellos.

Hoy en día existen tecnologías que permiten mayor privacidad, tales como la criptografía o los métodos de anonimato en Internet, y existen otras en cambio, que admiten mayor intrusión, como ser los dispositivos que recogen datos en la red de

manera sistemática e indiscriminada, el uso de un sniffer digital, los dispositivos de GPS, etc.

También se cuenta con cientos de miles de registros que día a día recolectan información personal –desde simples datos, hasta la imagen de un ser humano, su voz, las huellas digitales, etc.- que quedan en la web quizás de manera indefinida.

En concordancia, sostuvo la doctrina *"Para el profesor Spiros Simitis, las modernas formas de recolección masiva de datos personales han alterado la visión tradicional de la privacidad de tres formas concretas. Primero, las consideraciones sobre el derecho a la privacidad ya no afectan solamente a un sujeto en particular; se trata de conflictos que inciden sobre millones de individuos al mismo tiempo: se recolectan a diario datos personales de contribuyentes, de pacientes, de empleados, de clientes de banco, de ciudadanos, de beneficiarios de pensiones o de deudores. Segundo, numerosos dispositivos permiten almacenar y luego reconstruir con el mayor detalle posible cada uno de nuestros movimientos: tarjetas inteligentes, claves de acceso, GPS, celulares, número de identificación, entre muchos otros. Finalmente, toda esa información personal es utilizada cada vez más con mayor frecuencia para moldear estándares de comportamiento. La consecuencia de todo es que el almacenamiento y el posterior uso de datos personales se traducen en elementos esenciales para influenciar en la conducta de los individuos".*[13]

La solución encontrada para salvaguardar al individuo frente a dichos cambios sustanciales fue promulgar nuevas leyes. Por tal motivo, el derecho a la protección de la información personal puede definirse como *"un conjunto de reglas que guía a compañías y organizaciones en el uso que se hace de la información personal, es decir, la que identifica individuos o personas jurídicas. Son los estándares a aplicarse para el manejo de la información sobre las personas, y las practicas que deban seguirse para alcanzar y mantener esos estándares".*[14]

Tal como reguló el art. 1 de dicha ley, la finalidad de la norma en cuestión es la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos (sean públicos o privados) destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre ellas se registre.

Señaló Riquert que "*el hecho de que la disposición que señalamos aluda a "datos personales" no debe llevar a considerar que se refiere sólo a los pertenecientes a*

---

[13] Pablo A. Palazzi. Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388. Editorial Abeledo Perrot. Pág. 130.

[14] Pablo A. Palazzi. Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388. Editorial Abeledo Perrot. Pág. 130/131.

personas físicas, pues el art. 2 de la ley 25.326 define a aquellos como "la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables".[15]

Comparto la conclusión a la que arribaron los autores Tazza y Carreras quienes afirmaron que *"La presente modificación legal al sistema penal ha tenido el propósito fundamental de ajustar las disposiciones penales tradicionales a las nuevas formas de comunicación y al empleo de sistemas tecnológicos, recurriéndose para ello a una nueva definición del concepto de documento y de cosas pasibles de protección, extendiéndose la tutela del ordenamiento penal a aquellos objetos intangibles como el correo electrónico, las comunicaciones provistas por los sistemas de mensajería electrónica, el software, las páginas creadas y colocadas en internet, la información almacenada en soportes magnéticos o electrónicos, y otras aplicaciones surgidas a partir del incesante avance cibernético".*[16]

Siguiendo la misma línea de fundamento, argumentaron que *"Toda la información procedente de las nuevas formas tecnológicas de comunicación queda ahora especialmente alcanzada por la protección legal que se le otorgará a la correspondencia epistolar, las comunicaciones telefónicas y los papeles privados (arts. 153, 153 bis, 155 CP); a la vez que se ha receptado la figura de la intrusión en comunicaciones telefónicas y electrónicas dentro del mismo ámbito de protección. Del mismo modo se ha intensificado la cobertura penal respecto de toda la información personal que pudiese existir en un archivo o banco de datos personales, sancionando cualquier propalación indebida, al igual que su ilegitima intromisión y difusión (art. 157 bis C.P.)".*[17]

El segundo inciso de la citada ley definió al objeto del delito como aquel dato personal contenido en un soporte material (archivo). De acuerdo con esta norma, se lo considera el conjunto organizado de datos objeto de tratamiento o procesamiento, electrónico o no, cualesquiera que fueran las modalidades de su formación, almacenamiento, organización o acceso.

Para que la información suministrada sea considerada *"personal"* debe hacer referencia a ciertos aspectos de la vida del individuo, quedando encuadrados en dicha definición los datos sensibles vinculados a aquel.

En lo que refiere al bien jurídico que resulta más comprometido por las conductas punibles, puede mencionarse como prioridad la intimidad personal, entendida –y

---

[15] Marcelo A. Riquert. Protección Penal de la Intimidad en el Espacio Virtual. Editorial Ediar. Año 2003. Pág. 183/184.

[16] Alejandro O. Tazza y Eduardo Raúl Carreras. La protección del banco de datos personales y otros objetos de tutela penal. Cita online: AR/DOC/1782/2008. 20/08/2008. Editorial Thomson La Ley.

[17] Alejandro O. Tazza y Eduardo Raúl Carreras. La protección del banco de datos personales y otros objetos de tutela penal. Cita online: AR/DOC/1782/2008. 20/08/2008. Editorial Thomson La Ley.

potenciada por la constante evolución tecnológica- como el derecho del individuo a resolver sus cuestiones y tomar decisiones, al margen de la influencia de los otros.

Ya expresó la doctrina al respecto que *"El bien jurídico tutelado sigue siendo la intimidad de las personas, en especial, respecto de los datos personales almacenados en un sistema informático. Dicha tutela no excluye la afectación del servicio informático en sí, pero lo importante acá es proteger el uso extendido de los ordenadores en la vida cotidiana y el proceso de tratamiento y almacenamiento de la información ajena contenida en bancos de datos".*[18]

Asimismo, Buompadre sostuvo que *"estos delitos protegen la intimidad personal, entendida como espacio de reserva de los individuos necesario para el desarrollo de la personalidad y que el Estado debe preservar de toda intromisión ilícita por parte de personas no autorizadas".*[19]

En lo que atañe al delito mencionado en el art. 117 bis del Código Penal de la Nación, para desmenuzar la figura y su acción típica, debe destacarse que la idea de *"insertar"* alude a aquel sujeto que incluya datos falsos (no verdaderos) en un archivo de datos personales.

De igual forma *"hacer insertar"* está dirigido a quien logre que otra persona introduzca datos falsos en un archivo, lo cual puede efectuarse mediante cualquier medio idóneo que permita que dicha información quede registrada.

La inserción en cuestión debe ser ilegítima, es decir, debe ir en contra de la ley o sin la autorización de ella. Están pues, comprendidas en la disposición, las conductas de quien efectúe el registro a través de una computadora, un fichero, hojas movibles o por cualquier otro medio electrónico y/ o manual.

Primero y, antes que nada, debe ser distinguido de aquel previsto en el art. 239 del Código Penal de la Nación, ya que allí el objeto del delito se vincula a cualquier tipo de documento. Aquí, en cambio, se trata únicamente de las constancias de los datos personales contenidas en un registro (archivo).

Puede desprenderse del texto en cuestión, que la intención del legislador fue salvaguardar los datos personales por un lado y, por el otro, lograr la veracidad y la actualización de los contenidos de los registros y archivos.

La acción punible consiste entonces en proporcionar, esto es: dar, entregar, suministrar, poner a disposición, transmitir, etc., por cualquier medio (sea informático,

---

[18] Gustavo Eduardo Aboso. Código Penal de la República Argentina. Segunda edición actualizada. Comentado, concordado, con jurisprudencia. Editorial B de F. Montevideo/Buenos Aires. Año 2014. Pág. 780.

[19] Jorge E. Buompadre. Manual de Derecho Penal. Parte Especial. Editorial Astrea. Buenos Aires. Año 2013. Pág. 379.

oral, escrito, etc.) a un tercero una información falsa (a sabiendas de que lo es), la cual debe estar contenida en un archivo informático.

De acuerdo con la redacción del texto, pueden darse dos situaciones puntuales: proporcionar falsamente una información sobre un dato contenido en un archivo que se sabe que es falso, o bien, proveer como verdadera una información sobre un dato contenido en un archivo que se sabe que es falso.

Amans y Nager señalaron que *"se trataría de una modalidad específica del convencional delito de violación de secretos, generada por los avances tecnológicos".*[20]

La definición de *"falso"* se indica respecto de una realidad distinta a la que verdaderamente corresponde, sobre determinada persona física o jurídica. Se puede proponer que el dato falso se comunique como verdadero. Por supuesto que dicho falseamiento será de dolo directo, cualquiera sea la finalidad perseguida por el autor.

Con la actual redacción del texto se intentó tutelar la privacidad del sujeto que tiene registrada información personal en un archivo de datos de tal naturaleza. Por tal motivo, solo de manera secundaria podría verse lesionada la privacidad personal en sentido estricto, puesto que la información contenida en las bases de datos no se revela, ni se propaga, ni se proporciona a terceros, sino que se mantiene dentro de la misma esfera y ámbito de reserva, sólo que alterando o modificando indebidamente su correcta o autorizada versión informática de su contenido.

En conclusión, se protege la legalidad o el consentimiento de la información contenida en tales registros, más que la reserva o la privacidad personal de tales archivos.

La *figura básica* de este delito, para su configuración, no requiere que exista un perjuicio alguno para el sujeto pasivo o para terceros que tengan acceso. En contraposición, si la acción del sujeto produce algún menoscabo al titular del dato, se desplaza inmediatamente al *tipo agravado* (inciso tercero). Aquel puede ser de cualquier naturaleza y significación (patrimonial, moral o de otra naturaleza), pero cualquiera sea el caso, debe haber ocurrido efectivamente y recaer sobre una persona puntual, esto es, en el titular del dato o en un tercero damnificado.

La doctrina no perdió ello de vista al afirmar que *"Con la introducción de datos personales falsos o proporcionando información falsa de aquellos datos se puede disminuir o aumentar el patrimonio de una persona. Si se lo disminuye, es evidente que el perjuicio es para la persona sobre la que se está brindando información (por ejemplo, se niega la obtención de un crédito); pero si se aumenta, puede ocurrir que quien otorga*

[20] Carla V. Amans y Horacio S. Nager. Manual de Derecho Penal. Parte Especial. Editorial Ad Hoc. Buenos Aires. Año 2009. Pág. 219.

el crédito sea el perjudicado (se adjudica un crédito que a la postre puede resultar incobrable)".[21]

De igual manera, concordaron en que: *"Los perjuicios también pueden producirse a causa de los "usos secundarios" cuando los datos recogidos para determinado fin se utilizan con otra finalidad sin el consentimiento del consumidor. El uso secundario podría provocar daño psicológico derivado de un sentimiento de traición, especialmente si el consumidor tenía una expectativa razonable de que los datos fueran utilizados sólo para el objetivo original".*[22]

En cuanto al sujeto activo, no quedan dudas de que se trata de los usuarios que ingresan a la plataforma de los archivos y suministran la información simulada. Sin embargo, puede ampliarse la imputación también respecto de aquellos que tengan a su cargo el manejo o el tratamiento de la información que allí se introduce. En este último caso se trata de un tipo especial de autor calificado, pues sólo quien tiene el poder de disposición de dichos datos está en situación de proveerlos y únicamente el responsable o titular del archivo, registro, base o banco de datos se encuentra en aquella posición. De igual forma, el último inciso prevé la presencia de otro sujeto activo especial: el funcionario público en ejercicio de sus funciones.

El sujeto pasivo, en cambio, será la persona física o jurídica con relación a la cual se insertó indebidamente uno o más datos.

Tratándose de un delito de pura actividad y de peligro concreto, se consuma con la introducción del dato falso, por lo que no es necesario que el mismo haya sido divulgado. No admite la tentativa como posibilidad, pero sí cualquier forma de participación.

Cabe destacar en este punto, lo dicho por ciertos juristas reconocidos *"Steizel entiende que estos delitos también se pueden realizar mediante una omisión impropia. En estos casos, el sujeto activo es el responsable de la base de datos personales que no adopta los recaudos necesarios para prevenir que terceros, ajenos o no a la misma, puedan ingresar con el objeto de insertar datos falsos de una persona. El autor citado cree que ese sujeto se encuentra en una posición de garante respecto del bien jurídico tutelado penalmente, y que "si frente a la posibilidad concreta de evitar el resultado lesivo no realiza la conducta que lo evitaría (tomar medidas de seguridad, minimizar los riesgos, etcétera), entonces comete el delito previsto en el art. 117 bis del Cód. Penal.*

---

[21] Carlos A. Chiara Díaz. Código Penal y Normas Complementarias. Comentado, Concordado y Anotado. Arts. 54 al 139 bis. Tomo III. Editorial Jurídica Nova Tesis. Pág. 673.

[22] Yves Poullet, María Verónica Pérez Asinari y Pablo Palazzi. Derecho a la Intimidad y a la Protección de Datos Personales. Editorial Heliasta. Buenos Aires. Año 2009. Pág. 171.

Dicho de otra forma, a través de su omisión permite (no evita) la producción del resultado típico".[23]

Finalmente, hay que señalar que, existen dos posturas bien marcadas respecto de si la acción penal en este delito es pública y perseguible de oficio o si, por el contrario, es de instancia privada.

Con relación a la primera de ellas, ciertos doctrinarios sostuvieron que: *"La inclusión del art. 117 bis, en el título II del Código Penal., como figura que atenta contra el honor de las personas, no implica, sin la expresa modificación del art. 73 del Código Penal, que deba considerarse a las figuras previstas en aquel artículo, dependientes de acción privada. La enumeración del art. 73 es taxativa*".[24]

Apoyando tal idea manifestó la jurisprudencia: *"El delito de insertar o hacer insertar a sabiendas datos falsos en un archivo de datos personales, más allá de la ubicación de la figura en la hermenéutica del Código Penal y sin perjuicio de la intención que pudiera haber tenido el legislador, la interpretación de la norma debe partir de su propia literalidad, por lo que resulta posible atribuir responsabilidad penal en relación con ella a los propios titulares de la información personal contenida en los bancos de datos pertinentes. Ello es así, dado que el tipo legal no requiere que la información falsa desacredite o perjudique de algún modo a quien le es asignada, por lo que la acción típica puede darse por cumplida, también, cuando se obra para beneficiarlo. El delito en cuestión no se encuentra dentro de aquellos cuya acción es exclusivamente privada, en tanto no fue incluido en el artículo que, taxativamente, prevé los delitos de los que nace tal clase de acción (art. 73 del C.P.). En consecuencia, no es sólo el honor el bien protegido por el tipo de referencia, sino que son varios los bienes jurídicos que entran en cuestión, en tanto no resultaría lógico afirmar que el legislador ha querido que sea de acción pública un delito que afecta exclusivamente al honor y buen nombre de los ciudadanos, cuando, por otra parte, para los ilícitos que históricamente han estado referido a tales bienes (calumnias e injurias) se ha previsto que solo puedan juzgarse a partir de la acción privada*".[25]

En otro fallo se consideró que *"La inclusión del art. 117 bis, en el Título II como figura que atenta contra el honor de las personas, no implica, sin la expresa modificación del art. 73 de dicho ordenamiento, que deba considerarse a las figuras previstas en aquel artículo, dependientes de acción privada…" (Cam. Apel. Crim. Y Corr., Sala V,*

[23] David Baigún, Eugenio Raúl Zaffaroni y Marco Antonio Terragni. Código Penal y Normas Complementarias. Análisis Doctrinal y jurisprudencial. 4. Artículos 97/133. Parte Especial. Segunda edición actualizada y ampliada. Editorial Hammurabi. Buenos Aires. Año 2010. Pág. 428/429.

[24] Horacio J. Romero Villanueva. Código Penal de la Nación y Legislación Complementaria. Anotados con jurisprudencia. Editorial Abeledo Perrot. Buenos Aires. Año 2010. Pág. 461.

[25] CNACC, sala I, causa 26531_1, "Torres Sergio y otros", 07/12/2005.

11/12/02, causa 20.217 "C.N.A"). Los magistrados afirmaron en esa ocasión que la enumeración del art. 73 es taxativa, por lo que la circunstancia de que la ley 25.326 no haya incorporado modificación alguna a ese respecto veda la posibilidad de que en forma tácita pueda considerarse a la acción privada como requisito de procedibilidad, agregando que la redacción del art. 73 refiere a delitos en concreto y no a bienes jurídicos tutelados".[26]

En la doctrina nacional podemos encontrar una opinión similar. Steizel afirmó que *"Si bien los otros dos delitos previstos en el mismo Capítulo se encuentran dentro de los delitos de acción privada, el legislador optó por no incluir al delito incorporado en el art. 117 bis dentro de éstos, colocándolo consecuentemente junto a los delitos de acción pública. Lo que resulta coherente puesto que, como expresáramos supra, por ser un delito de peligro abstracto no es necesaria una víctima concreta".*[27]

En contraposición, la otra corriente alude a que, según surge de la interpretación del código, es el propio damnificado quien tiene la obligación de tomar las riendas de su perjuicio y se apoya en los veredictos donde ya se estipuló que *"(…)habiéndose ubicado aquellos en el presente capitulo ("Violación de secretos"), estamos frente a un delito de acción privada, ya que, si el legislador hubiera querido incluirlos en las excepciones que prevé el inc. 2 del art. 73 ("los casos de los arts. 154 y 157") así lo habría previsto expresamente en la ley 25.326, que los incorporó al código de fondo*".[28]

Haciendo alusión a lo expresado por intelectuales como Baigún, Zaffaroni y Terragni *"Para aquellos que sostenemos que las figuras que contiene el tipo penal del art. 117 bis son una clase del delito de injurias (en este caso, agravadas), entendemos que no resulta necesaria una modificación a la enumeración del art. 73 del Cód. Penal, desde el momento en que en el inc. 1° de esa norma se hace expresa referencia a esta clase de delito. Para sostener esta postura encontramos una razón de índole sistemática: los demás ilícitos previstos en el título "De los delitos contra el honor (arts. 113, publicación o reproducción de injurias o calumnias proferidas por otro; 114, calumnia o injuria propagada por medio de prensa: 115, injurias proferidas por las partes en un juicio y 116, injurias recíprocas), no se encuentran enumerados en el inc. 1° del art. 73 y, a pesar de ello, nadie duda de que éstos sean de acción privada debido a que son conductas relacionadas con los delitos de calumnia e injuria. Consecuentemente, el*

---

[26] David Baigún, Eugenio Raúl Zaffaroni y Marco Antonio Terragni. Código Penal y Normas Complementarias. Análisis Doctrinal y jurisprudencial. 4. Artículos 97/133. Parte Especial. Segunda edición actualizada y ampliada. Editorial Hammurabi. Buenos Aires. Año 2010. Pág. 434.

[27] David Baigún, Eugenio Raúl Zaffaroni y Marco Antonio Terragni. Código Penal y Normas Complementarias. Análisis Doctrinal y jurisprudencial. 4. Artículos 97/133. Parte Especial. Segunda edición actualizada y ampliada. Editorial Hammurabi. Buenos Aires. Año 2010. Pág. 434/435.

[28] CNACC, sala IV, causa 2.079/11_4, "Sabaris Di Lorenzo, Javier A.", 08/03/2012.

delito contenido en el art. 117 bis (al tratarse de una injuria) se encuentra enmarcado en la enumeración taxativa del inc. 1° del art. 73 del Cód. Penal. De tal forma, atendiendo a la particular naturaleza de los delitos de acción privada, éstos no deben iniciarse ni impulsarse de oficio, sino sólo por interposición de querella por parte del ofendido (de conformidad con lo establecido en los arts. 7, 415 y ss. del Cód. Procesal Penal de la Nación)".[29]

La norma descripta en el art. 157 bis, en *el primer inciso* reprime el acceso ilegitimo. Es decir que el sujeto que ingresa debe carecer de permiso o autorización para ello y por lo general, esto se efectúa mediante la utilización de un programa que violenta el sistema de seguridad.

Tal como lo definió el diccionario de la Real Academia Española *"acceder"* es tener acceso, paso o entrada a un lugar, sin que se necesiten medios especiales, es decir, que quien ingresa al objeto de protección puede hacerlo por vía de una computadora o por cualquier otro medio electrónico.

Lo que la ley pretende reprimir particularmente, es el acceso indebido; es decir, el que no se haya realizado inadvertida o casualmente y por lo general mediante el uso de sistemas de comunicaciones.

El autor, quien puede ser cualquier persona ya que no requiere cualidad especial (delito común) debe actuar de una manera dolosa al acceder de manera no autorizada a una base pública o privada de datos personales.

El sujeto pasivo, en cambio, es aquella persona física o institución, pública o privada, que resulta titular del banco de datos.

El objeto de la figura son los datos que ya están registrados o guardados confidencialmente por una ley. Así, el acceso en violación de sistemas de confidencialidad se considera efectuado por quien no es un usuario con su debida clave, ni una persona debidamente autorizada al efecto. En este caso, el intruso burla a la protección dada por el servidor y a todo el marco que gira alrededor de la debida seguridad o de los niveles de protección.

El delito se consuma con el mero acceso al sistema, por lo que no se requiere el apoderamiento de la información allí inserta. La esfera de reserva se vulnera atacando al banco mismo y quebrantando así las seguridades con que se lo ha dotado para impedir el conocimiento de terceros.

---

[29] David Baigún, Eugenio Raúl Zaffaroni y Marco Antonio Terragni. Código Penal y Normas Complementarias. Análisis Doctrinal y jurisprudencial. 4. Artículos 97/133. Parte Especial. Segunda edición actualizada y ampliada. Editorial Hammurabi. Buenos Aires. Año 2010. Pág. 435.

Cabe destacar que admite la tentativa, cualquier forma de participación y una parte de los autores sostienen que se trata de un delito formal, de pura actividad y de peligro abstracto *"puesto que se consuma con el solo hecho de acceder, sin necesidad de la divulgación de los datos ni de que se cause perjuicio, real o potencial".*[30]

En *el segundo* inciso se regula la conducta del confidente necesario infiel. La información debe ser procesada y almacenada por personas que, necesariamente, debido a su profesión u oficio, se interiorizan o tienen acceso a las bases de datos en cuestión.

Para la Real Academia Española *"proporcionar o revelar"* se trata de poner a disposición de alguien lo que necesita, actuar que equivale a suministrar, dar o entregar. Revelar, lo mismo que descubrir, es poner la información registrada en el archivo en conocimiento de una persona que no lo posee.

Este confidente necesario tiene el deber de reserva (art. 10 de la citada ley), el cual solo cede ante la intimidación judicial o por razones fundadas de seguridad pública, defensa nacional o salud pública.

Por lo expuesto, la figura en estudio no exige un acceso indebido, ya que el propio confidente necesario está legalmente habilitado para el tratamiento de esa información. Lo que veda es la conducta de brindar la información a terceros que no están habilitados para su conocimiento.

La acción de proporcionar incluye tanto a la entrega de un soporte material con los datos personales reservados, como a permitir el ingreso de una tercera persona al sistema.

A diferencia del apartado anterior, este sí que es un delito especial, ya que autor de la maniobra solo será el confidente necesario.

Al respecto, puede mencionarse cierto dictamen donde se trabajó ese punto y se dispuso que *"(…) revelar indica descubrir, poner a la luz algo que se encontraba oculto" (Carlos Parma. Habeas Data. El artículo 157 del Código Penal. En: Martínez R., Juan Carlos, Delitos de blanqueo y lavado de activos, en el marco de operaciones sospechosas. Notas sobre la Ley Nro. 19.913, que crea la Unidad de Análisis Financiero, 2002, Buenos Aires. El autor. págs. 43 a 56)". "Se trata de esta manera que el hecho, documento o actuación sea comunicado a una tercera persona, fuera círculo de quienes tienen derecho o les corresponde conocerlo". "Sobre la base de estas consideraciones, y en relación con el caso de marras, debemos mencionar que el artículo 10 de la ley de Habeas Data (nro. 25.326) dispone que "el responsable y las personas que intervengan*

[30] Carlos Fontán Balestra. Tratado de Derecho Penal. Parte Especial. Tomo II. Edición Actualizada y Ampliada. Editorial La Ley. Pág. 472.

en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos".[31]

Finalmente, *en el tercer inciso* se reprime a la acción típica de insertar o hacer insertar ilegítimamente cierta información en un archivo de datos personales. Esto incluye a la acción dolosa de la persona que directamente lo inserta, como a aquel que determina a otro a su inserción.

La norma se refiere a insertar datos, pero no aclara cuáles pueden ser. El resultado típico requerirá entonces que el archivo se modifique, ya sea agregándose nuevos asientos o borrando los preexistentes.

El autor debe actuar con dolo directo y en nada influye para su configuración que los datos a los que hace alusión sean verdaderos o falsos. Igual que en el inciso anterior, sólo será un confidente necesario el habilitado para dicha tarea, ya que por lo general demanda una actualización de estos.

A su vez, admite la tentativa y todas las formas de participación. He de decir que, para cualquiera de los incisos, la figura se agrava por la calidad del sujeto activo en su calidad funcionarial, fundamento de la aplicación de la pena de habilitación que se suma a la de prisión ya regulada.

Tal circunstancia alude en forma directa e inmediata al art. 77 del Cód. Penal, el cual se amplió por lo dispuesto mediante la llamada *"Ley de Ética de la Función Pública*" (nro. 25.188) la cual en su art. 1 instauró que *"La presente ley de ética en el ejercicio de la función pública establece un conjunto de deberes, prohibiciones e incompatibilidades aplicables, sin excepción, a todas las personas que se desempeñen en la función pública en todos sus niveles y jerarquías, en forma permanente o transitoria, por elección popular, designación directa, por concurso o por cualquier otro medio legal, extendiéndose su aplicación a todos los magistrados, funcionarios y empleados del Estado. Se entiende por función pública, toda actividad temporal o permanente, remunerada u honoraria, realizada por una persona en nombre del Estado o al servicio del Estado o de sus entidades, en cualquiera de sus niveles jerárquicos".*

Se trata de una agravante condicionada solamente a la calidad del autor, es decir, que revista el carácter de funcionario público. Para habilitar la mayor penalidad es suficiente con la sola cualificación del sujeto activo, sin que se requiera que al momento del hecho se encuentre en ejercicio de dicha actividad pública.

En lo que atañe a la competencia, el art. 44 de la ley nro. 25.326 sienta la jurisdicción federal respecto de los registros, archivos, bases y bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional, de modo que –en tales casos- corresponderá asignar la competencia al fuero de excepción.

---

[31] CNACCF, sala I, causa 40462, "Prieto Manuel E. s/ nulidad", 11/10/2007.

CUARTA PARTE: La órbita de protección de los datos personales en el derecho Internacional

- **La Organización de las Naciones Unidas**

Los comienzos de la protección de los datos personales se remontan al año 1948, momento a partir del cual la Asamblea General de las Naciones Unidas adoptó el documento conocido como "*Declaración Universal de Derechos Humanos"*, en el cual se expresaron los derechos humanos conocidos como básicos para cualquier ser humano del mundo. [32]

En el art. nro. 12 señaló lo siguiente: "*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".*

En consecuencia, la privacidad empezó a considerarse como lo que es, un valor totalmente esencial para el desarrollo de cada ser humano, de su personalidad y para la protección de su dignidad, tema central que se aborda a lo largo de todo ese documento.

Tal derecho busca protegernos de las interferencias injustificadas en nuestra vida –ya sea de personas y/o de diferentes organismos- y llegar así a determinar cómo queremos nosotros interactuar con el mundo y con la sociedad que nos rodea.

Es una política que trata de ofrecer un marco claro para garantizar la dignidad humana y los derechos de todas las personas, incluso en esta era totalmente masiva y digital, que sus redactores -al momento de formularla- jamás pudieron prever.

En tal sentido no puedo dejar de destacar los dichos pronunciados por la Alta Comisionada para los Derechos Humanos -Michelle Bachelet- quien sostuvo en una de sus conferencias que deben arbitrarse los medios necesarios para lograr un trabajo en conjunto entre los abogados de derechos humanos, los informáticos, los ingenieros y los representantes de los gobiernos, con el objeto de garantizar la continua aplicación de los derechos humanos sobre la forma en que los Estados operan en la era digital y regulan las actividades de las empresas en el espacio digital. [33]

---

[32] Gabriel Sánchez Pérez e Isaí Rojas González. Leyes de protección de datos personales en el mundo y la protección de datos biométricos – Parte I. Publicado en Revista Seguridad (http://revista.seguridad.unam.mx/print/2124. Consultado el día 07/06/2020).

[33] Artículo 12: derecho a la intimidad. Página Oficial de las Naciones Unidas. Publicado el 21/11/2018 (http://news.un.org/es/story/2018/11/1446671. Consultado el día 07/06/2020).

En la misma línea se pronunció el relator especial de la Comisión ante el Consejo de Derechos Humanos -Joseph Cannataci-[34], quien manifestó que el ciberespacio depende de la voluntad y capacidad de los Estados de trabajar juntos para lograr la sinergia entre la privacidad y la seguridad.[35]

- **El Parlamento Europeo y el Consejo de la Unión Europea**

El reglamento nro. 2019/679 del Parlamento Europeo y del Consejo (UE) entró en vigor el 25 de mayo de 2016, pero fue aplicado recién en el año 2018, periodo durante el cual las empresas, las organizaciones, los organismos y las instituciones debieron ir adaptándose a su cumplimiento.

Se trató de una normativa relativa a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, a nivel de la Unión Europea, con jurisdicción en las empresas con origen en ella, como en las que tienen negocios dentro del bloque –aunque se encuentren físicamente por fuera-.

Uno de los requisitos insertos fue que, para poder utilizar la información allí suministrada de un sujeto en particular, resulta imprescindible contar con su expreso consentimiento, mediante un acto que demuestre su manifestación de voluntad libre para tal fin, ya sea por escrito (incluyendo medios electrónicos), tildando una casilla en un sitio web o con una declaración verbal.

A su vez, determinó que las entidades que manipulen los datos en cuestión deberían acreditar que fueron recabados de manera legal, licita, transparente y con un fin determinado, que se recopilaron de la forma adecuada que sean utilizados para lo estrictamente necesario, como así también que estén actualizados, seguros y que sean mantenidos únicamente durante el tiempo que fueran necesarios.

Estipuló la inserción de la figura del *"delegado"* para referirse a quien esté encargado de supervisar, informar y asesorar respecto del cumplimiento de la normativa, sujeto que deberá tener una formación adecuada para ejercer la función y contará con los recursos necesarios para realizarla. No podrá ser destituido o sancionado sin motivo alguno.

Permitió que los ciudadanos puedan solicitar que sus reseñas sean suprimidas cuando ya no resulten necesarias a la finalidad paran la que fueron recogidas, se haya retirado el consentimiento o se sepa que se han utilizado de manera ilícito. También logró que ella se recupere para luego retransmitirlas a otra entidad.

---

[34] Declaración del Relator Especial sobre el Derecho a la Privacidad tras visitar Argentina. Página oficial de las Naciones Unidas en Argentina. Publicado el 17/05/2019. Buenos Aires (http://www.onu.org.ar/declaracion-del-relator-especial-sobre-el-derecho-a-la-privacidad-tras-visitar-argentina/. Consultado el día 07/06/2020).

[35] Las políticas de ciberseguridad, una amenaza contra la intimidad. Página Oficial de las Naciones Unidas. Publicado el 07/03/2018 (http://news.un.org/es/story/2018/03/1428622. Consultado el día 07/06/2020).

Puntualizó que, si la empresa llegara a tomar conocimiento de una violación en el uso de la información, tendrá un plazo máximo de 72 horas para notificar a la autoridad competente y al afectado de tal circunstancia.

Destacó también que no será necesaria la autorización previa para exportar datos a terceros países u organizaciones internacionales, si se hace acorde a las cláusulas aprobadas por la Comisión Europea. Pese a ello, los flujos fronterizos de datos no podrán en ningún caso implicar un menoscabo en el nivel de protección.

Para tal fin creó el *"Consejo Europeo de Protección de Datos"* formado por los representantes de cada una de las 28 autoridades de control independientes, el cual puede adoptar decisiones jurídicamente vinculantes.

- **Budapest**

El Convenio de Cibercriminalidad del año 2001 obligó en el art. 2 a los Estado Parte que lo suscribieron, a que adopten las medidas necesarias legislativas –o de otro tipo- para prever como infracción penal, conforme a su derecho interno, el acceso doloso y sin autorización a toda o a una parte de un sistema informático.

Sumado a ello aclaró que pueden exigir que dicha infracción sea cometida con vulnerabilidad de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva.

Por otra parte, en el art. 4, impuso que se castigue la conducta de dañar, borrar, deteriorar, alterar o suprimir los datos informáticos, dolosamente y sin autorización.

- **España**

La Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) nro. 15/1999 acompaña al RGPD UE 2016/976 y se encuentra vigente desde el 13 de diciembre de 1999.

Con la última modificación confeccionada el 25 de mayo del 2018 provocó grandes cambios. En efecto, a partir de allí se eliminó el concepto del consentimiento tácito por parte de los involucrados en los registros de datos, lo que generó que, desde aquel momento, sí o sí se deba realizar de manera expresa y tal circunstancia debe ser verificable por la entidad involucrada. Agregó que, a partir de aquel momento, los menores de 13 años pueden participar, pese a que previamente era desde los 14 años.

También registró que para evitar riesgos las entidades tendrán que utilizar un fuerte cifrado para proteger de manera jurídica y real los datos de sus clientes. A tal fin designaron a un *"delegado"*, el cual debe ser informado a la Agencia Española de Protección de Datos.

Por otra parte, aplicó el principio de transparencia para que los afectados, en caso de verse vulnerados, puedan tomar conocimiento del mal uso de su información.

Promovió la existencia de mecanismos de autorregulación en el sector público y privado, introduciendo para ello la obligación de bloquear la información, lo que permitió garantizar que todo lo realizado quede a disposición de las autoridades, un tribunal o el Ministerio Fiscal y evitar de esta forma que se borre lo efectuado para encubrir su posible incumplimiento.

Al respecto, se expidió el tribunal supremo al decir que: *"El art. 3 a) de la Ley Orgánica de protección de datos de carácter personal (LOPD) concreta el concepto de "datos de carácter personal" como "cualquier información concerniente a personas físicas identificadas o identificables". La letra c) del mismo precepto define el "tratamiento de datos" como las "operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias"; "(...)el articulo 2 a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995(...)entiende por dato personal "toda información sobre una persona física identificada o identificable (el interesado); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social"; "Estamos, en definitiva, dentro del núcleo esencial del derecho fundamental del art. 18.4 CE, que se actualiza aún de modo más notorio cuando, como en el caso a examen, nos encontramos en un ámbito(...)que ofrece múltiples medios de tratamiento de los datos; sistemas, por lo demás, en auge y desarrollo exponencial, que se amplía y perfeccionan a un ritmo vertiginoso y que se añaden a otros más conocidos"; "(…)el art. 18.1 CE impone como regla de principio y, de forma añadida al resto de las garantías(...)un deber de información que protege frente a intromisiones ilegítimas en la intimidad. Es inequívoca en ese sentido, por ejemplo, la STC 196/2004, de 15 de noviembre, FJ 9, según la cual "se vulnera el derecho a la intimidad personal cuando la actuación sobre su ámbito propio y reservado no sea acorde con la ley y no sea consentida, o cuando, aun autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida".; "(...)"la función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquél ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad.(...)En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado...Pero ese poder de disposición sobre los*

propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen y con qué fin"; "(...)es complemento indispensable del derecho fundamental del art. 18.4 CE "la facultad de saber en todo momento quién dispone de esos datos personales y a que uso los está sometiendo"; "Ese derecho de información opera también cuando existe habilitación legal para recabar los datos sin necesidad de consentimiento, pues es patente que una cosa es la necesidad o no de autorización del afectado y otra, diferente, el deber de informarle sobre su poseedor y el propósito del tratamiento. Es verdad que esa exigencia informativa no puede tenerse por absoluta, dado que cabe concebir limitaciones por razones constitucionalmente admisibles y legalmente previstas"; "Y es que privada la persona de aquellas facultades de disposición y control sobre sus datos personales, lo fue también de su derecho fundamental a la protección de datos, toda vez que, como concluyó en este punto la STC 11/1981, de 8 de abril (FJ 8), "se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección".[36]

Con posterioridad a ello, volvió a desarrollar aquellos argumentos en otro fallo, refiriendo que *"el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Esos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos"; "Son así elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales(…)el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y,*

[36] TC, 2712, "Fraile Nieto Adolfo Tomás s/ amparo", 12/03/2013

en su caso, requerirle para que los rectifique o los cancele" (STC 292/2000, de 30 de noviembre, FJ 7)"; "(…)el art. 6.1 LOPD prevé que "el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado salvo que la ley disponga otra cosa"".

"El deber de información sobre el uso y destino de los datos personales que exige la Ley Orgánica de protección de datos de carácter personal está íntimamente vinculado con el principio general de consentimiento para el tratamiento de los datos, pues si no se conoce su finalidad y destinatarios, difícilmente puede prestarse el consentimiento".[37]

Si bien este conjunto de normas no contiene delitos punibles para dichas acciones, el art. 197 del Código Penal Español es extenso con relación a las faltas que se vinculan con la privacidad y con la información personal. A través de seis incisos, esta norma detalla en forma muy amplia diversos delitos contra la privacidad y la confidencialidad.

Dispone en el primer inciso, la pena de prisión de uno a cuatro años –y multa de doce a veinticuatro meses- para aquel que descubra los secretos o vulnere la intimidad de otro sin su consentimiento, como así también para quien se apodere de papeles ajenos, cartas, mensajes de correo electrónico o cualquier otro documento similar, efectos personales, intercepte telecomunicaciones, utilice artificios de escucha, transmisión grabación o reproducción del sonido y de la imagen o de cualquier otra señal de comunicación.

En el segundo apartado sanciona con igual pena a quien, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de un tercero, datos reservados de carácter personal o familiar de otro, que se hallen registrados en ficheros, soportes informáticos, electrónicos o telemáticos, como así también en cualquier otro registro público o privado.

De igual forma penaliza a quien, sin estar autorizado, acceda por cualquier medio a dicha información, los altere o utilice en perjuicio del titular o de un tercero.

Estipula que las penas serán agravadas si la información descripta es revelada, ya sea por parte del autor o de un tercero, si la maniobra es realizada por las personas encargadas o responsables de los ficheros, si tal circunstancia se hace con un fin de lucro o cuando las acciones recaen sobre datos sensibles (ausente en nuestra legislación).

- **Alemania**

La Ley Federal de protección de datos (Bundesdatenschutzgesetz – BDSG) está considerada un sistema de auto regulación por no poseer un registro central de datos.

[37] TC, 3405, "Rodríguez Liberato Mónica Rebeca s/ amparo", 08/04/2016.

El aspecto principal de su creación fue permitir el procesamiento de los datos solamente si el derecho lo permite, o si el particular ha dado su consentimiento.

De la sección nro. 44 surgió la pena de prisión de hasta dos años o de multa a la persona que venda datos de un tercero, a cambio de dinero, con la intención de enriquecerse o para perjudicar a alguien más.

Aquel apartado detalló las faltas que pueden cometerse en dicho ámbito, tanto con dolo o por negligencia, como ser: recolectar datos personales que no son accesibles sin autorización, poner a disposición de terceros datos personales que no son accesibles sin autorización y obtener datos personales a través de información incorrecta o desleal.

Con fecha 25 de mayo del año 2018 se realizó una modificación dentro de la norma, que trajo aparejada una gran rigurosidad en comparación a las disposiciones exigidas previamente en el reglamento del Parlamento Europeo y del Consejo 2019/679.

En puntual, se dispuso que aquellas firmas que operan en aquel país deben designar a un funcionario para la protección de los datos en aquellos casos donde se empleen al menos diez personas con habitualidad y se ocupen del tratamiento automatizado de datos personales.

Por otra parte, nombró a un oficial de protección de estos, cuando por ejemplo se procese comercialmente esa información para fines de transferencia (personal o anónima) o para propósitos de investigación de mercado u opinión, debiendo tomar las medidas apropiadas para que la vigilancia, los nombres de los controladores y los datos de contacto se identifiquen inmediatamente en el sistema.

Asimismo, en lo que atañe a la carga de la prueba frente a algún reclamo de quien se sienta afectado por la intromisión a su vida privada mediante este medio, se estipuló que sean las empresas quienes tendrán que demostrar que cumplen con las normas vigentes para proteger la información en cuestión.

De igual forma, para defenderse frente a demandas civiles de las multas regulatorias y de los sujetos de datos, se reguló que deberán ser capaces de documentar sus esfuerzos para lograr el cumplimento de la ley, debiendo adaptar para ello tanto los sistemas, como la documentación respectiva para que se les permita poder probar qué datos personales corresponden a cada sujeto especifico que procesaron, como para qué fines se utilizaron y mediante qué medios.

Otro cambio significativo para tener en cuenta fue que los comités creados dentro de las compañías cumplirían sí o sí a partir de aquel momento con los reglamentos dispuestos, lo que no resultaba necesario previo a dicha metamorfosis.

De lo expuesto, se desprende que este modelo evidencia una problemática existente ya que no demuestra cómo la autoridad nacional podría percatarse o tomar conocimiento de la existencia de pequeñas bases de datos que pudieran infringir los principios reconocidos internacionalmente, teniendo en cuenta que sólo podrán

intervenir luego de recibir una queja por parte del particular que ya se haya visto directamente perjudicado.[38]

- **Inglaterra**

La Ley de Protección de Datos inglesa -en su sección nro. 55- penaliza a quien ilegítimamente y sin la autorización del responsable del tratamiento obtenga o revele datos personales o la información contenida en ellos, o procure la revelación de información a otra persona.

Asimismo, agrega que constituye una ofensa punible la venta de datos personales si fueron obtenidos en contracción a dicha sección.

Resulta interesante señalar que la norma se refiere al consentimiento del responsable del tratamiento y no del titular de los datos en cuestión. Lo que el texto legal buscó titular, no fue la privacidad de aquel (aunque lo haga de manera indirecta), sino evitar que esta información caiga en las manos incorrectas.

Lo expuesto está vigente desde el año 1998 pero, en el año 2006, el Comisionado de Protección de Datos propuso aumentar las penas para estos delitos con el objeto de atacar al mercado ilegal. Dicho supuesto está contenido en el art. 76 de la ley *"Criminal Justice and Inmigration Bill"* la cual designó la pena de custodia para cualquier segunda condena por violación a la ley de protección de datos y, en concreto, para aquellos sujetos que compren y vendan datos personales ajenos.

- **Unión Africana**

La Convención de la Unión Africana (UA) sobre Ciberseguridad y Protección de Datos Personales, regulada en junio del año 2014, tiene como objetivo armonizar las legislaciones preexistentes sobre seguridad cibernética en todos los Estados miembros de la Unión Africana –incluyendo la legislación procesal penal- y establecer en cada uno de ellos un mecanismo capaz de combatir las violaciones del derecho a la intimidad.

De igual forma, llamó a establecer un marco normativo coherente con el entorno jurídico, cultural, económico y social de África. Ofreció protección contra amenazas en línea, hechas contra una persona sobre la base de la raza, el color, la ascendencia, el origen nacional-étnico o la religión.

A su vez, reivindicó la coherencia con la Carta Africana sobre los derechos humanos y de los pueblos, pero la carta, a diferencia de esta Convención, incluyó al sexo en la lista de clases protegidas, omisión notable y preocupante en la presente.

[38] Protección de Datos en Alemania. Leyderecho.org. Publicado 04/2018 (https://leyderecho.org/proteccion-de-datos-en-alemania/. Consultado el día 07/06/2020).

El mayor inconveniente que se vislumbra es que los gobiernos africanos podrían aprovechar las amplias excepciones de la Convención para restringir el procesamiento de datos personales en nombre del *"interés público"* o del *"ejercicio de la autoridad oficial"* de manera arbitraria. Estos términos no se definieron correctamente en el documento aludido y, por ende, cabe la posibilidad de que se utilicen luego para justificar el abuso de las entidades gubernamentales en tal sentido.

La Convención postuló la prohibición de hacer, difundir o descargar el contenido que contenga amenazas o insultos con una base en la raza, el color, la ascendencia, el origen nacional-étnico o la religión. Aquello hace eco en el Protocolo sobre la Xenofobia y el Racismo añadido en el Convenio del Consejo de Europa sobre Delitos Cibernéticos.[39]

- **Estados Unidos**

Se trata de un país donde las normas y las reglas para el tratamiento de los datos privados varían según el estado, lo que da lugar a diferentes niveles de seguridad y exigencias dependiendo de dónde opere cada empresa, por lo que no se puede hablar de una única forma de proteger la información.

A nivel federal, en el año 1998 se aprobó una norma conocida como *"Identity Theft and Assumption Deterrence Act",* que penalizó el uso no autorizado de identificación de terceros, pero no permitió formular un reclamo a la entidad financiera, sino sólo al autor del robo de identidad. A su vez, cuarenta y cuatro estados en este país penalizaron el robo de identidad como un delito autónomo.

Sumado a ello, en noviembre del año 1999 se aprobó la Ley de Modernización Bancaria (conocida también por los apellidos de los legisladores que la redactaron: los senadores Gramm, Leach y Bliley), la cual propuso un conjunto de normas federales sobre la privacidad en dicha rama y estableció nuevos delitos que penalizaron la adquisición fraudulenta de información sobre los clientes.

Su creación fue la respuesta del Congreso a los escándalos ocurridos durante aquellos años con los llamados *"information brokers",* quienes, en forma desleal, con pretextos y excusas falsas, obtenían datos personales y económicos de los clientes bancarios para venderlos a terceros o para cometer delitos como podría ser el robo de la identidad.

Cabe destacar que hace aproximadamente dos años creció la polémica en torno a este asunto, cuando el último presidente electo, Donald Trump, firmó una ley para

[39] Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales. *Leyderecho.org*. Publicado 04/2018 (http://leyderecho.org/convencion-de-la-union-africana-sobre-ciberseguridad-y-proteccion-de-datos-personales. Consultado el día 07/06/2020).

permitir que los proveedores de servicios de internet –más allá de las firmas Facebook y Google que ya estaban autorizados con anterioridad a ello- vendieran los datos de los consumidores sin su consentimiento previo.

En lo que respecta a la legislación estatal, la ley de California aprobada en el año 2002 (y en vigor desde el año 2003) fue la primera en su tipo, ya que definió cuando las agencias de bases de datos comerciales y otras empresas deben notificar las fallas que permiten la adquisición -por una persona no autorizada- de información personal no pública y no cifrada con relación a un residente de aquel estado.

Para ellos *"la información personal"* integra el nombre de la persona y algún otro dato que podría consistir por ejemplo en el número de seguridad social, de licencia de conducir, de una tarjeta de crédito, una cuenta bancaria, etc. Así, para el año 2005, casi la mitad de los estados ya habían adoptado leyes de notificación.

Posteriormente, en el año 2018 surgió otra discusión luego de promulgarse la Ley de Privacidad del Consumidor de California (California Consumer Privacy Act - CCPA), la cual entró en vigor en enero del corriente año, que cambió radicalmente todo este asunto, brindando a los consumidores derechos de privacidad expansivos y un mayor control sobre la información personal que las empresas recopilan sobre ellos, asemejándose en parte a lo estipulado en el GDPR europeo.

A partir de dicha modificación, las empresas debieron identificar los datos personales previamente recolectados, su naturaleza, identificar el propósito del tratamiento, los datos cedidos y los vendidos, lo que los obligará a la constante actualización de los registros.

No puedo dejar de hacer alusión a la visión del sistema descripto, por parte de la doctrinaria española Saldaña en una de sus publicaciones, donde sostuvo que: *"(...)a lo largo de todo el siglo XX, la protección de la esfera privada en los Estados Unidos ha pasado del ámbito del common law al propio del Derecho constitucional, como consecuencia de su evolución desde una noción propietaria de la privacidad (privacy-property) a una concepción estrechamente relacionada con la dignidad de la persona, consolidándose como un bien jurídico fundamental merecedor de la máxima protección en el sistema constitucional norteamericano"; "(...)el derecho de la privacidad es un concepto amplio, que va más allá del derecho a la intimidad vigente en el ámbito europeo.(...)al delimitarse progresivamente los intereses constitucionales que lo integran, esto es, aquellos ámbitos de la esfera privada que tienden a preservar esos intereses de soledad, secreto, autonomía, individualidad, intimidad, desarrollo de la personalidad, libertad de elección en asuntos personales, control de la información personal, así como del sustrato esencial de la inviolable dignidad humana".*

Continuo con el desarrollo de su postura, manifestó que*"(...)en la Sociedad de la Información y del Conocimiento de principios del siglo XXI(...)se ha definido el derecho a la privacidad como el poder de controlar el flujo de información personal y como el derecho a decidir cuándo, cómo y en qué medida la información personal es comunicada a otros, proceso de autodeterminación personal que ha de integrarse asimismo en los procesos comunicativos y participativos en los que interviene el individuo"; "A partir de 1974(...)se aprueba la primera ley general de protección de la información personal en poder de las Agencias Federales de los Estados Unidos, la llamada Privacy Art"; "(...)la "zona de privacidad" protegida constitucionalmente no sólo ampara la autonomía individual en la toma de decisiones importantes sino también el "interés" individualmente en evitar la revelación de asuntos personales"; "(...)en 1980, el Tribunal de Apelaciones del Tercer Circuito señaló en United States v. Westinghouse Electric Corporation(...)los elementos a considerar para decidir si una intromisión en la privacidad individual está justificada son el tipo de datos solicitados, la información que contiene o puede contener, el potencial daño en una subsiguiente revelación no consentida, la existencia de garantías que prevengan revelaciones no autorizadas, el grado de necesidad de acceso, y si hay un mandato legal expreso, política pública u otro interés público reconocible que canalice el acceso.(...)estableció que la información médica pertenece al ámbito de la privacidad merecedor de protección en la medida en que contiene datos íntimos de naturaleza personal";*

Finalmente, puso su énfasis en que*"(...)los Tribunales han aplicado un exigente escrutinio para admitir la constitucionalidad de la revelación de información personal contenida en archivos confidenciales médicos, como la vida sexual privada, la orientación sexual, los informes psicológicos o el padecimiento del SIDA"; "(...)el Tribunal Supremo norteamericano parece anclado en el pasado y manifiesta una evidente resistencia a hacer frente al ineludible tratamiento constitucional complejo que exige la protección de los derechos de la privacidad en la sociedad tecnológica avanzada de principios del siglo XXI, en la que el Estado dispone de tecnología y facultades para obtener, almacenar y utilizar información de carácter personal en amplias bases de datos, información que puede ser muy sensible, crucial para la recuperación y el bienestar personal, cuya filtración puede generar daños irreparables, que, sin duda, deben ser evitados por la Constitución. Sin olvidar la amenaza que suponen las tecnologías destructivas de la privacidad individual implementadas gracias a la red telemática mundial que representa Internet".*[40]

[40] María Nieves Saldaña. El derecho a la privacidad en los Estados Unidos: Aproximación diacrónica a los intereses constitucionales en juego. Publicado en el portal Dialnet. Fecha de aceptación: 29/07/2011.

- **Bolivia**

El Código Penal del año 1997, específicamente en el art. 363 ter., prevé la alteración (la modificación, la supresión o la inutilización) y el uso indebido de datos informáticos (el acceso y el apoderamiento) –sin autorización- con relación a los alojados en una computadora o en cualquier soporte informático.

- **Colombia**

A partir de la modificación del Código Penal, mediante la ley nro. 1273 del año 2009, se incorporó un capítulo específico respecto de la delincuencia informática. Concretamente, en el art. 269 castigó a quien –sin autorización- ingrese a un sistema informático protegido, o no, mediante una medida de seguridad, o se mantenga dentro de aquel en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.

- **Uruguay**

La ley nro. 18.331 sancionada con fecha 11 de agosto del año 2008, le reconoció a la protección de datos personales un estatus de derecho humano fundamental, inherente a los sujetos y lo aplicó por extensión a las personas jurídicas.

Hizo alusión a la estrecha guarda del secreto profesional, para quienes se encuentran obligados en tal sentido, debido de su profesión.

A su vez creó como organismo de control *"La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento, a cuyo cargo está la potestad sancionatoria administrativa".*

- **Venezuela**

En el capítulo III de la LECDI del año 2001, puntualmente en el art. 20, el legislador penó a quien intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, si en consentimiento de su dueño, la data o información personal de alguien más, o sobre las cuales tenga interés legítimo, los cuales estén incorporados en una computadora o un sistema que utilice tecnologías de información.

- **Paraguay**

El Código Penal del año 1997, en su art. 174 sanciona a quien lesione el derecho de disposición de otra persona, sobre sus datos, al borrarlos, suprimirlos, inutilizarlos o cambiarlos y en los apartados siguientes penó a quien altere a los datos en cuestión.

Dicha disposición entiende como *"datos"* a aquellos que sean almacenados o se transmitan electrónica o magnéticamente, o en otra forma inmediatamente visible.

- **Perú**

La alteración, el daño y la destrucción a una base de datos se incorporó al Código Penal del año 1991 mediante la ley nro. 27.309, con fecha 17 de julio del año 2000, la cual fue finalmente derogada por la ley nro. 30.096 del año 2013, la cual en el art. 3 se refirió al atentado contra la integridad de los datos informáticos.

CONCLUSION

Para redondear la idea expuesta a lo largo de todo el presente trabajo, sugiero que nos hagamos las siguientes preguntas: ¿Es viable evitar el acceso indebido a los sistemas informáticos de los centros asistenciales de la salud?; ¿puede el Sistema Integrador de Historias Clínicas Electrónicas y el Registro de Historias Clínicas Electrónicas de la Ciudad Autónoma de Buenos Aires, garantizar y asegurar la privacidad de los pacientes? Pienso que, basándome principalmente en la información recolectada a lo largo de este trabajo y en todo lo aquí expuesto, la respuesta es un rotundo no.

Lo cierto es que, con el avance constante e intermitente de la tecnología, de la internet y de los dispositivos masivos que contienen datos, los cuales avanzan y se perfeccionan día a día, resulta imposible para el hombre acomodarse a estas nuevas realidades, ya que se actualizan más deprisa aun que las propias normas que lo protegen luego de ellas y de la profunda intromisión a la vida privada que conllevan.

Pese a ello, gracias a diversas leyes -tanto locales como nacionales- que fui mencionando a lo largo del presente (nro. 1845, 5669 y 25.326 de la Ciudad Autónoma de Buenos Aires, nro. 26.529 y art. 19 de la Constitución Nacional) se logró ir adecuando nuestro sistema de salud a esta nueva era digital, en concordancia con el derecho fundamental de todos los hombres a resguardar su privacidad, intentando así proteger la información contenida en las bases de datos, principalmente en las historias clínicas digitales.

Sin embargo, no puede negarse que existen diversos casos -y seguirán existiendo- en los cuales se producen ingresos indebidos a los registros médicos (por parte de terceras personas, autorizadas o no) que perjudican indefectiblemente al titular de los datos allí consignados, ya sea porque modifican su contenido, los borran, los utilizan con fines personales y/o comerciales, etc.

En tal sentido, para los casos previamente mencionados, o para cualquier otro que encuadre en tales maniobras, nuestra legislación prevé las figuras incluidas en los artículos 157 bis del Código Penal de la Nación, y 117 bis del Código Penal de la Nación (modificado por el art. 32 de la ley 25.326), que penan a aquellos sujetos que manipulan la información suministrada en las historias clínicas digitales y al sistema de mención, ya sea ingresando correctamente desde aparatos tecnológicos de dichas instituciones,

o mediante la comisión de algún tipo de delito informático, con el objeto de utilizar dichos datos maliciosamente o con algún provecho personal y/o económico.

Asimismo, quiero hacer fundamental hincapié en otro supuesto que no podemos desconocer, ya que sucede con habitualidad, como es el caso de la industria de los seguros médicos (obras sociales, prepagas, etc.), donde en más de una oportunidad también acceden a la información en cuestión y luego la utilizan para excluir a ciertas personas del servicio que ofrecen, amparándose en diversos motivos, como ser ciertos antecedentes familiares de enfermedades crónicas, genéticas o predisposiciones varias, circunstancias que los dejan por fuera del estándar mínimo requerido para que dichas entidades puedan protegerles la salud, por ser sujetos más propensos a acarrear mayores enfermedades que el resto de la población. Considero que deberíamos replantearnos si los requisitos excluyentes para obtener un cuidado médico (indispensable para vivir) pueden estar basados en datos personales y sensibles, o si debiesen establecerse según datos más generales de cada ciudadano.

Por otra parte, tal como puede observarse en el capítulo que alude al derecho internacional, los retos de las nuevas tecnologías obligaron a cada país a reformular sus normas, con la finalidad de proteger este derecho esencial como es la intimidad, circunstancia que dejó en evidencia la dificultad que aparece en este nuevo marco global.

Ahora bien, considero que quizás como sociedad todavía no tomamos dimensión de las enormes consecuencias que el nuevo desarrollo tecnológico trae aparejado y lo vislumbramos únicamente como un gran avance, dejando de lado la reflexión crucial de sí nuestro derecho a la intimidad, tal cual como lo conocemos hasta ahora, puede ser incluido en el nuevo mundo moderno, el cual sin lugar a duda trae consigo nuevas formas de vulneración de este derecho.

Cabe preguntarnos entonces si los mecanismos jurídicos con los que contamos en la actualidad son suficientes, o sí, por el contrario, debiéramos reformular las herramientas que tenemos para resguardarnos de este acelerado avance.

Para ello, a lo largo de este trabajo, traté de dejar siempre en evidencia que debemos hacer valer nuestro derecho fundamental a la intimidad, el cual se encuentra en peligro frente a la volatilidad de nuestra información personal, como resultado de la gran cantidad de aplicaciones y plataformas tecnológicas que se incorporan con total normalidad a nuestra vida cotidiana.

BIBLIOGRAFIA

- Aboso. G. E. Código Penal de la República Argentina. Segunda edición actualizada. Comentado, concordado, con jurisprudencia. Editorial B de F. Montevideo/Buenos Aires. Año 2014.
- Aboso. G. E. La inconstitucionalidad de la requisa y el examen sin autorización judicial de datos personales almacenados en dispositivos celulares de personas detenidas. Publicado en elDial.com – DC1D2F- el 31/07/2014.
- Amans, C. V. y Nager, H. S. Manual de Derecho Penal. Parte Especial. Editorial Ad Hoc. Buenos Aires. Año 2009.
- Artículo 12: derecho a la intimidad. Página Oficial de las Naciones Unidas. Publicado el 21/11/2018 (http://news.un.org/es/story/2018/11/1446671. Consultado el día 07/06/2020).
- Baigún, D., Zaffaroni, E. R. y Terragni, M. A. Código Penal y Normas Complementarias. Análisis Doctrinal y jurisprudencial. 5. Artículos 134/161. Parte Especial. Editorial Hammurabi, Buenos Aires. Año 2008.
- Baigún, D., Zaffaroni, E. R. y Terragni, M. A. Código Penal y Normas Complementarias. Análisis Doctrinal y jurisprudencial. 4. Artículos 97/133. Parte Especial. 2da edición actualizada y ampliada. Editorial Hammurabi, Buenos Aires. Año 2008.
- Buompadre, J. E. Manual de Derecho Penal. Parte Especial. Editorial Astrea. Buenos Aires. Año 2013.
- Caramelo, G. Historia Clínica. Página oficial del Ministerio de Salud y Desarrollo Social de la Nación. Publicado 03/2017 (http://www.salud.gob.ar/dels/entradas/historia-clinica. Consultado el día 07/06/2020).
- Chiara Díaz, C. A. Código Penal y Normas Complementarias. Comentado, Concordado y Anotado. Arts. 54 al 139 bis. Tomo III. Editorial Jurídica Nova Tesis.
- Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales. Leyderecho.org. Publicado 04/2018 (http://leyderecho.org/convencion-de-la-union-africana-sobre-ciberseguridad-y-proteccion-de-datos-personales. Consultado el día 07/06/2020).
- Creus, C. y Buompadre, J. E. Derecho Penal. Parte Especial. Tomo I. 7ª edición actualizada y ampliada. Editorial Astrea. Buenos Aires. Año 2007.
- Declaración del Relator Especial sobre el Derecho a la Privacidad tras visitar Argentina. Página oficial de las Naciones Unidas en Argentina. Publicado el 17/05/2019. Buenos Aires (http://www.onu.org.ar/declaracion-del-relator-especial-sobre-el-derecho-a-la-privacidad-tras-visitar-argentina/. Consultado el día 07/06/2020).
- Fontán Balestra, C. Tratado de Derecho Penal. Parte Especial. Tomo II. Edición Actualizada y Ampliada. Editorial La Ley.

- González Fuster, G. TEDH – Sentencia de 04.12.2008, S. y Marper C. Reino Unido, 30562/04 y 30566/04 – Artículo 8 CEDH – Vida privada – Injerencia en una sociedad democrática – Los límites del tratamiento de datos biométricos de personas no condenadas. Revista de Derecho Comunitario Europeo. ISSN 1138-4026, núm. 33. Madrid. Mayo/agosto 2009.
- Justicia Cerca. Mi Historia Clínica. Portal Oficial del Estado Nacional Argentino (http://www.argentina.gob.ar/justiciacerca/historia-clinica. Consultado el día 07/06/2020).
- Las políticas de ciberseguridad, una amenaza contra la intimidad. Página Oficial de las Naciones Unidas. Publicado el 07/03/2018 (http://news.un.org/es/story/2018/03/1428622. Consultado el día 07/06/2020).
- Orihuela, A. M. Constitución Nacional Comentada. Sexta Edición. Editorial Estudio. Año 2012.
- Palazzi, P. A. Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388. Editorial Abeledo Perrot.
- Patitó, J. A. Manual de Medicina Legal. Segunda edición. Editorial Librería Akadia. Buenos Aires. Año 2012.
- Poullet, Y., Pérez Asinari, M. V. y Palazzi, P. Derecho a la Intimidad y a la Protección de Datos Personales. Editorial Heliasta. Buenos Aires. Año 2009.
- Protección de Datos en Alemania. Leyderecho.org. Publicado 04/2018 (https://leyderecho.org/proteccion-de-datos-en-alemania/. Consultado el día 07/06/2020).
- Quiroga Lavié, H. Constitución de la Nación Argentina Comentada. Segunda edición actualizada. Editorial Zavalia. Año 1997.
- Riquert, M. A. Acceso ilegitimo a banco de datos personales, revelación ilegitima de su información e inserción ilegitima de datos (art. 157 bis, CP). Revista de Derecho Penal y Criminología. Editorial Thomson Reuters. Publicado en febrero del 2015.
- Riquert, M. A. Protección Penal de la Intimidad en el Espacio Virtual. Editorial Ediar. Año 2003.
- Romero Villanueva, H. J. Código Penal de la Nación y Legislación Complementaria. Anotados con jurisprudencia. Editorial Abeledo Perrot. Buenos Aires. Año 2010.
- Saldaña Diaz, M. N. El derecho a la privacidad en los Estados Unidos: Aproximación diacrónica a los intereses constitucionales en juego. Publicado en el portal Dialnet. Fecha de aceptación: 29/07/2011.
- Sánchez Pérez, G. y Rojas González, I. Leyes de protección de datos personales en el mundo y la protección de datos biométricos – Parte I. Publicado en

Revista Seguridad (http://revista.seguridad.unam.mx/print/2124. Consultado el día 07/06/2020).

- Tazza, A. O. y Carreras, E. R. La protección del banco de datos personales y otros objetos de tutela penal. Editorial Thompson La Ley. Cita Online AR/DOC/1782/2008. Publicado el 20/08/2008.