La Protección Penal de los Datos Personales

En Argentina el resguardo legal de la intimidad históricamente estuvo suficientemente garantizado por la Constitución Nacional (arts. 19 y 18) y los Códigos Civil (art. 1071 bis) y Penal (arts. 151 al 157 relativos a la violación del domicilio y de secretos).

Pero todo cambió a fines del siglo XX ya que con el uso masivo de los nuevos sistemas electrónicos de comunicación, antes desconocidos, la intimidad, la identidad y el anonimato de las personas se vieron crecientemente amenazados. Además, surge una nueva idea: la del *derecho a la protección de los datos personales* (conocido también como "*autodeterminación informativa*"), como derecho distinto y más evolucionado que los de confidencialidad y privacidad. Si bien la privacidad sigue ocupando un rol central en la protección de datos personales, existen múltiples intereses tutelados por esta última, que además están relacionados con la calidad, intangibilidad y exactitud de la información, su seguridad y la forma en que las organizaciones tratan los datos personales.

Para dar respuesta a esta nueva realidad, en el año 2000 se sancionó la Ley Nº 25.326 de Protección de Datos Personales. Su finalidad fue salvaguardar integralmente los datos de carácter personal que se encontrasen en registros o bancos de datos, para así poder garantizar tanto el derecho al honor y a la intimidad de las personas, como el derecho de controlar la información que sobre las mismas se registre.

La ley 25.326 introdujo en el derecho argentino el concepto de *dato personal*, como objeto de tutela jurídica y reglamentó a su vez la acción constitucional de hábeas data (incorporada en la Constitución Nacional con la reforma de 1994). Introdujo, asimismo, modificaciones al Código Penal, que a su vez fue reformado nuevamente por la ley 26.388/08.

Los conductas típicas que afectan la Protección de Datos personales están incluidas en el capítulo "Violación de Secretos y de la Privacidad". Su colocación, además de ilustrar acerca de cuál es el bien jurídicamente protegido, permite clasificar a estos delitos como de *acción privada*.

"157 bis. Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años".

Analizaremos en detalle cada una de las acciones punibles:

1- Acceso no autorizado a Banco de Datos Personales:

Se pena el acceso, cualquiera sea la forma en que se realizó. No se especifica la modalidad de ingreso de tal forma que no sería necesario un medio informático.

La redacción de este inciso es incorrecta, si observamos que la violación de sistemas de confidencialidad y la violación de sistemas de seguridad de datos son claramente medios con los que puede accederse ilegítimamente al banco de datos personales, pero no son los únicos.

Es un delito Doloso, el agente debe haber obrado a sabiendas de que su acceso era ilegítimo. La ilegitimidad importa la falta de consentimiento.

El delito, que admite tentativa, se consuma con el mero acceso al banco de datos personales.

2- Proporcionar o revelar información registrada en un Banco de Datos Personales:

Se pena proporcionar o revelar la información a otra persona, cuando por disposición de la ley estuviere obligado a preservar su secreto. Se excluyen así las bases de datos de uso público, que no están sujetas a confidencialidad.

La LPDP establece quiénes son los obligados a confidencialidad:

- El responsable del banco de datos;

- Todos los que intervengan en cualquier fase del procesamiento, aún después de finalizada la relación con la actividad de la base de datos. Incluiría a los propios usuarios y a terceros que tratan temporariamente los datos.

Para ser típica la conducta debe ser ilegítima. No lo es cuando los datos son revelados o proporcionados cumpliendo con la Ley de Protección de Datos Personales. Tampoco cuando los agentes son relevados de su deber de secreto mediante resolución judicial o cuando medien razones de seguridad o salud públicas, o cuando se pudiere afectar la defensa nacional.

Es un delito doloso, se consuma con la simple revelación o proporcionar la información y no requiere que se produzca ningún daño.

3- Inserción de datos en un banco de datos personales:

Se reprime la inserción de los datos, con prescindencia de que sean verdaderos o falsos. Si lo que se hiciera fuere destruir o dañar, se configuraría el delito de Daño.

Sujeto activo del delito puede ser cualquier persona ajena –o no- al banco de datos, que actúe por sí o a través de un tercero.

Es una figura dolosa, que admite tentativa.

Finalmente, para todos estos delitos, el artículo prevé una pena adicional de inhabilitación cuando el sujeto activo fuere un funcionario público.

El Código Penal español agrava también estos injustos en los casos en que el autor fuere encargado o responsable del fichero, cuando los datos fueren sensibles y cuando se obrare con fines de lucro.

Daño

La alteración, destrucción o inutilización de bases de datos personales también es reprimida por el Código Penal, de igual modo que lo hace la legislación española.

El bien jurídico protegido es la *propiedad*.

183 C.P.: *"Será reprimido con prisión de quince días a un año (...) el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños"*.

Las conductas punibles son:

Alterar: es cambiar la esencia, modificar el dato, sin destruirlo.

Inutilizar: hacer que el archivo que contiene el dato deje de funcionar, también sin destruirlo.

Destruir: borrar el archivo sin posibilidad de que sea recuperado.

Es un delito Doloso, que admite tentativa y la acción es pública.

Se reprime con una pena mayor cuando los datos fueran públicos.

A diferencia de las normas de España y Luxemburgo, la LPDP incluye bajo su regulación también a los archivos, registros o bases de datos personales no electrónicos, de modo que éstos pueden ser también objeto de daño, que también se agravará cuando se tratare de un archivo público.

La regulación en Paraguay guarda similitud con la argentina, pero expresamente aclara que por “dato” se entenderá al transmitido electrónica o magnéticamente o en otra forma no inmediatamente visible.

La Transmisión ilegal de bases de datos.

La transmisión ilegal de bancos de datos no fue tipificada por nuestro Código Penal, como sí hacen otras legislaciones. Sin embargo la apropiación ilegítima de una base de datos puede encuadrar, según el caso, en las figuras de Hurto o Robo.

A continuación analizaremos las legislaciones penales de varios países de América Latina. En general, advertimos que la privacidad está reconocida como derecho constitucional y se han previsto acciones para que los ciudadanos accedan a la información que sobre ellos obren en registros públicos o privados.

Son pocos los países que han previsto tipos penales especiales que protejan a los *datos personales*, pero de todos modos reciben tutela con figuras como la Violación de Secretos o las figuras que se refieren a “datos” en general.

México:

El Código Federal Penal mexicano ha tipificado los delitos relacionados con la interceptación de comunicaciones, el acceso ilícito a los sistemas de cómputo y el daño informático.

Regula en un capítulo especial el Acceso ilícito a sistemas y equipos de informática, sin hacer mención en ningún momento a los bancos de datos personales. Sumamente clara es la redacción de este capítulo, que podría sistematizarse del siguiente modo:

En todos los casos, estamos frente al acceso a sistemas o equipos de informática. La sanción varía si el acceso se realiza burlando algún mecanismo de seguridad que los protege o estando autorizado.

Se reprime a quien indebidamente:

- Modifique, destruya o provoque pérdida.
- Conozca o copie (o utilice) información.

Si los sistemas o equipos son del Estado o pertenecen a las instituciones del sistema financiero, las penas se agravan. También cuando se trate de equipos de seguridad pública.

Asimismo, prevé una agravante cuando la información obtenida se utilice en provecho propio o ajeno.

En el Código Penal argentino se reprime el mero acceso indebido (es un delito de peligro), pero esta figura es desplazada por los tipos especiales ya estudiados, cuando se trata de datos personales.

Perú

De manera similar a la normativa mexicana, el Código Penal peruano sanciona al que utiliza o ingresa indebidamente a una base de datos, a un sistema o red de computadoras o a cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos.

Si la finalidad con que actuó el agente fue alterar, dañar o destruir una base de datos, un sistema, una red o un programa de computadoras, la pena es mayor.

El delito se agrava si el sujeto activo accede a una base de datos, sistema o red de computadoras, haciendo uso de información privilegiada, obtenida en función a su cargo o pone en peligro la seguridad nacional.

Bolivia

Reprime en un artículo el apoderamiento, acceso, utilización, modificación, supresión o inutilización de datos almacenados en un medio informático, cuando cause

un perjuicio al titular de la información. No hace un tratamiento aparte para los datos personales, pero protege la inviolabilidad de las comunicaciones privadas.

Chile

La Ley 19.223 sobre Delincuencia Informática reprime los delitos de: sabotaje informático, espionaje informático, alteración de datos, incluida su destrucción o daño, y la revelación o difusión no autorizada de datos contenidos en un sistema de tratamiento de información.

Uruguay

No cuenta con una ley específica sobre delitos informáticos. La Ley 16.736 equipara a los delitos de falsificación de documentos públicos tipificados en el Código Penal con la transmisión voluntaria de un texto del que resulte un documento infiel, la adulteración o destrucción de un documento almacenado en soporte magnético, o su respaldo, utilizando medios informáticos y telemáticos.

Resulta criticable que sólo se mencione el soporte magnético –y no al digital-. En todo el Código Penal no figura ni una vez la palabra “dato”.

Colombia

El Código Penal colombiano sí tiene una regulación específica para la violación de datos personales.

Pune a la persona que, sin estar facultada para ello, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

Las acciones pueden ser realizadas en provecho propio o de un tercero.

Observamos aquí una diferencia importante con la legislación argentina, que no castiga penalmente la venta de datos personales en forma ilegal (aunque esta actividad puede constituir un ilícito civil y administrativo).

Paraguay

No legisló figuras penales directamente relacionadas a la afectación de los datos personales, que por lo tanto reciben tutela con los artículos del Código Penal que castigan la lesión a la intimidad de la persona (que tiene prevista pena de multa).

Legisla asimismo delitos cometidos a través de medios informáticos. Reprime la alteración de datos, el sabotaje de computadoras y su utilización para cometer fraudes. De acuerdo a su ubicación, los bienes jurídicamente protegidos serían "los bienes de las personas" y las "relaciones jurídicas".

Venezuela

Dentro del capítulo dedicado a los delitos contra la privacidad de las personas y de las comunicaciones, el Código Penal tipifica el apoderamiento, utilización, modificación o eliminación, sin el consentimiento de su dueño, de la *data o información personales* de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información.
El delito se agrava si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.
También reprime la revelación indebida de data o información de carácter personal, aún cuando el autor no hubiese tomado parte en su obtención.
Prevé una pena mayor si la difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro.

La Convención de Budapest sobre Delitos Informáticos

La Convención de Budapest sobre Delitos Informáticos o Convenio sobre Ciberdelincuencia es un acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre delitos informáticos (derecho penal, derecho procesal y cooperación internacional). Fue adoptada por el Consejo de Europa en noviembre de 2001y entró en vigor el de julio de 2004. Este convenio es el único que se encarga de la seguridad de la información y trata los delitos contra la Confidencialidad, Integridad y Disponibilidad de los datos y los sistemas informáticos.

La República Argentina expresó su voluntad este año adherir al convenio, sin embargo, desde antes ya viene adecuando su legislación penal a las directrices que emanan de este tratado.

Concretamente, los Estados signatarios deberán prever en su derecho interno como infracción penal a:

- Acceso ilícito a un sistema informático;
- Interceptación ilícita de datos durante su transmisión;
- Dañar, borrar, deteriorar, alterar o suprimir dolosamente datos informáticos.

Fija luego principios relativos a la Extradición, que será viable cuando los Estados implicados hayan previsto una pena de una duración mínima de un año de privación de la libertad para las infracciones recién mencionada.

Aquellos Estados que tengan prevista una pena mínima distinta, derivada de un tratado de extradición, aplicarán la pena mínima prevista en esos tratados o acuerdos.

Los Estados se comprometerán a incluir a estas infracciones como susceptibles de dar lugar a extradición en todos los tratados de extradición que puedan suscribir.

Si un Estado condiciona la extradición a la existencia de un tratado y recibe una demanda de extradición de otro Estado con el que no ha suscrito tratado alguno de extradición, podrá considerar el presente Convenio fundamento jurídico suficiente para conceder la extradición por alguna de las infracciones penales mencionadas.

Juan Ignacio Aime.