El día 14 de agosto del corriente, se aprobó la Ley 20.327 sobre la prevención y represión de la Ciberdelincuencia.

La mencionada Ley, tiene como base la tipificación de los ciberdelitos, y la regulación y prevención para combatir los mismos, lo cual constituye un avance en la regulación de actividades ilícitas mediante el uso de medios telemáticos.

Por otra parte, brinda a las instituciones financieras y las entidades emisoras de dinero electrónico, a crear registros de ciberdelincuentes y a realizar medidas de prevención respecto a transacciones no consentidas.

A continuación, se detallan los puntos introducidos por el proyecto, el cual supone un avance significativo, en tanto se trata de delitos que además de carecer de regulación, su número ha ido in crescendo debido al avance tecnológico y la democratización su acceso.

Capitulo 1) La tipificación de ciberdelitos

El proyecto de Ley es novedoso, en cuanto a la tipificación que realiza de los ciberdelitos, la cual no existía hasta la fecha. Dentro de esta figura delictual, se encuentran los siguientes:

- Acoso telemático
- Fraude informático
- Daño informático
- Acceso ilícito a datos informáticos
- Interceptación ilícita
- Vulneración de datos
- Suplantación de identidad
- Abuso de dispositivos

Se trata de dos grupos de delitos, el primero destinado a proteger la integridad física y psíquica del sujeto vulnerado, y el segundo grupo destinado a proteger la seguridad y confidencialidad de datos.

1.1 Acoso telemático (Art. 288 BIS)

Acerca del acoso telemático, se prevé como sujeto activo como cualquiera que mediante el uso de dichos medios "desarrolle en forma insistente cualquiera de las siguientes conductas", dichas conductas son: "vigile, persiga o procure cercanía física, estableciendo o intentando establecer contacto con una persona, sea de forma directa o por medio de terceros"

La pena establecida es de tres meses de prisión a tres años de penitenciaria, y se establece como circunstancia agravante especial del delito, cuando el mismo se constituya en detrimento de un menor de edad, de adultos incapaces, de personas que hayan tenido una relación afectiva, o de individuos en situación de vulnerabilidad, ya sea por enfermedades u otras circunstancias de vida.

En concordancia con lo anterior, con la aprobación de la ley 19.580 se agregó al Código Penal Uruguayo el art 277 BIS, por el cual se castiga con 6 meses de prisión a cuatro años de penitenciaria, a " el que, mediante la utilización de tecnologías, de internet, de cualquier sistema informático o cualquier medio de comunicación o tecnología de trasmisión de datos, contactare a una persona menor de edad o ejerza influencia sobre el mismo, con el propósito de cometer cualquier delito contra su integridad sexual, actos con connotaciones sexuales, obtener material pornográfico u obligarlo a hacer o no hacer algo en contra de su voluntad será castigado con de seis meses de prisión a cuatro años de penitenciaría"

1.2 Fraude informático (Art. 347 BIS)

El Fraude informático implica la realización de estratagemas o engaños artificiosos a efectos de inducir en error para obtener información, o bien la ejecución de manipulaciones informáticas, en ambos casos con el fin de realizar operaciones financieras no consentidas en perjuicio de otro. Asimismo implica la utilización de cualquier medio de pago y/o datos vinculados a los mismos para realizar cualquier operación no consentida, previéndose una

pena de seis meses de prisión a cuatro años de penitenciaria, previéndose como agravantes -entre otras- la vinculación laboral o afectiva y/o que el hecho se efectúe en perjuicio del Estado.

A partir de la Ley No. 20.327 de prevención y represión de la Ciberdelincuencia, se incluye dentro de la lista de actividades delictivas precedentes del delito de lavado de activos, el delito de "Fraude informático" incorporado a la legislación mediante el Art. 347 BIS del Código Penal, siempre que "el monto real o estimado sea superior a 200.000 UI".

El delito de lavado de activos requiere que existan bienes que procedan de actividades delictivas precedentes cometidas con anterioridad al mismo (cuya integración al sistema formal se pretende lograr con dicho proceso). Tales actividades se encuentran establecidas taxativamente por la ley, específicamente en el art. 34 de la Ley Integral contra el lavado de activos No. 19.574.

1.3 Daño informático (Art. 358 QUATER).

Requiere la destrucción o inutilización de datos o sistema informáticos, con la finalidad de causar un daño.

Es decir, que a efectos de configurar el delito es necesario además de la acción, que se cometa con dolo.

1.4 Acceso ilícito a datos informáticos (Art. 297 BIS)

Para que se configure el delito, la acción debe realizarse sin autorización y sin justa causa. El articulo pena las siguientes conductas: "acceda, interfiera, difunda, venda o ceda información ajena contenida en soporte digital"

1.5 Interceptación ilícita (Art. 297 TER)

La acción tipificada como delito consiste en la "interrupción o interferencia" por medios técnicos, de datos informáticos en transmisiones no públicas, dirigidas a un sistema informático.

1.6 Vulneración de datos (Art. 297 QUATER)

Prevé una pena de 6 a 24 meses de prisión, para quien mediante el uso de cualquier medio telemático "acceda, se apodere, utilice o modifique datos confidenciales de terceros".

Este articulo implica un gran avance respecto a la protección de datos confidenciales, generando mas garantías para los usuarios.

1.7 Suplantación de identidad (Art 347 TER)

En la era de las redes sociales, este articulo adquiere suma relevancia, ya que pena a quien " que usurpe, adopte, cree o se apropie de la identidad de otra persona física o jurídica, valiéndose de cualquier medio, herramienta tecnológica o sistema informático, obteniendo datos accediendo a redes sociales, casillas de correo electrónico, cuentas bancarias, medios de pago, plataformas digitales, o cualquier credencial digital o factor de autenticación, con la intención de dañar a su legítimo titular".

A su vez, indica expresamente que no constituye una suplantación de identidad, la creación de un perfil destinado a la parodia.

1.8 Abuso de dispositivos (Art. 358 QUINQUIES).

Refiere a la producción, adquisición, importación, comercialización o facilitación de sistemas informáticos o telemáticos de cualquier índole, credenciales o contraseñas de acceso a datos informáticos o sistemas de información. A efectos de configurar el delito, dicha acción debe estar destinada inequívocamente a la comisión de un delito.

2) Medidas educativas

En el segundo capitulo del Proyecto de Ley, se establece la promoción de una campaña educativa acerca de ciberseguridad y el manejo de finanzas personales, en todos los centros dependientes de la Dirección General de Educación Secundaria de la Direccion General de Educación Técnico Profesional.

Asimismo, comprenderá a beneficiario de prestaciones de BPS, CEIBAL y los programas de INEFOP.

El fin de estas medidas, además de promover la educación y conocimiento acerca de los distintos conceptos, tales como "medios de pago", "acceso a financiamiento (prestamos,

análisis de tasas de interés, plazos), "planificación presupuestaria", entre otros, es evitar los fraudes tendientes al acceso de datos personales y financiero.

Dentro de las medidas educativas, se propone que la sociedad tome conocimiento de los siguientes términos: phishing, vishing, smishing, malware, troyano e ingeniería social.

3) Registro de ciberdelincuentes.

Se faculta a las instituciones de intermediación financiera y a las entidades emisoras de dinero electrónico a crear registros interinstitucionales que contengan datos para identificar, gestionar y prevenir transacciones no consentidas, así como operativas fraudulentas.

4) Transacciones no consentidas

Se faculta a su vez a las instituciones de intermediación financiera y a las entidades emisoras de dinero electrónico, a la no ejecución de cualquier orden de retiro o transferencia de activos brindada por personas físicas o jurídicas titulares o apoderados de cuentas, cuando hubieren tomado conocimiento que en las cuentas referidas, ingresaron fondos de terceros a través de transacciones declaradas como desconocidas y/o no autorizadas por el titular de las cuentas de origen de los fondos transferidos.

Se dispone que la inmovilización de fondos alcanzara hasta el limite del monto de las transacciones denunciadas como desconocidas, y no autorizadas por el titular.

Es decir que, la medida es aplicable tanto a saldos actuales como a futuros ingresos, siempre y cuando se trate de la transacción denunciada como desconocida.

Por otra parte, se establece que en caso de efectivizarse la inmovilización de fondos, deberá ser comunicada dentro del plazo de un día hábil al Banco Central del Uruguay, el cual podrá solicitar información adicional a las instituciones financieras en caso de ser necesario.

Se prevé a su vez, una serie de situaciones por las cuales la institución podrá dejar sin efecto la inmovilización de fondos. En ese caso, debe realizarse la comunicación al BCU.

5) Conclusiones

La aprobación de esta Ley marca un antes y un después en la regulación de los ciberdelitos en Uruguay, acompasando la normativa interna con los estándares internacionales, tales como la Convención de Budapest de 2001 (la cual no ha sido ratificada aun por nuestro país).

Entendemos de gran relevancia el hecho de la incorporación del delito de Fraude informático, dentro del elenco de delitos precedentes del lavado de activos, así como la incorporación de las agravantes al acoso telemático, acompasándose a lo establecido en la Ley 19.580.

Si bien aún queda camino por recorrer en lo referido a los ciberdelitos tanto a nivel nacional como internacional, la aprobación del proyecto marca un avance en su prevención y en consecuencia, su combate.