C/1734/2021

N° 552

La Cámara de Representantes de la República Oriental del Uruguay, en sesión de hoy, ha sancionado el siguiente

Proyecto de Ley

CAPÍTULO I

TIPIFICACIÓN DE CIBERDELITOS

Artículo 1º.- Agréganse al Capítulo I del Título XI del Libro II del Código Penal, los siguientes artículos:

"ARTÍCULO 288 BIS. (Acoso telemático).- El que mediante la utilización de medios telemáticos desarrolle de forma insistente cualquiera de las siguientes conductas, será castigado con tres meses de prisión a tres años de penitenciaría: vigile, persiga o procure cercanía física, estableciendo o intentando establecer contacto con una persona, sea de forma directa o por intermedio de terceros, de tal modo que altere gravemente el desarrollo de su vida".

"ARTÍCULO 288 TER. (Circunstancias agravantes especiales del delito de acoso telemático).- Será circunstancia agravante especial del delito de acoso telemático que se constituya en detrimento de un menor de edad, de adultos incapaces, de personas que previamente hayan tenido una relación afectiva o íntima, o de individuos vulnerables por enfermedad o por situaciones especiales que supongan una mayor fragilidad".

Artículo 2º.- Agrégase al Capítulo IV del Título X del Libro II del Código Penal, el siguiente artículo:

"ARTÍCULO 277 TER. (Circunstancias agravantes especiales del delito previsto por el artículo 277 BIS).-

A) Que las actividades descriptas en el tipo se ejecuten mediante coacción, intimidación o engaño hacia los menores de edad.

B) Que el hecho sea realizado por personas con un vínculo de afinidad o parentesco con el menor.

C) Que el contacto se realice con un menor de trece años de edad, con discapacidad, deficiencias físicas o psíquicas".

Artículo 3º.- Agréganse al Capítulo III del Título XIII del Libro II del Código Penal, los siguientes artículos:

"ARTÍCULO 347 BIS. (Fraude informático).- Se considera autor de fraude informático y será castigado con la pena prevista en el artículo 347, a quien incurra en alguna de las siguientes conductas:

A) El que, con estratagemas o engaños artificiosos, induzca en error a alguna persona para obtener información mediante tecnologías de la información y de la comunicación para procurarse, a sí mismo o a un tercero, un provecho injusto en daño de otro.

B) Efectúe manipulaciones informáticas o artificios afines con el fin de realizar operaciones financieras, transferencias o pagos no consentidos en perjuicio de otro, independientemente de que el beneficio sea personal o de un tercero.

C) Utilice cualquier tipo de tarjeta, cheque, código o cualquier otro medio de pago, o los datos vinculados a los mismos, para realizar transferencias, pagos o cualquier operación no consentida, con el fin de obtener un provecho en daño de otro".

"ARTÍCULO 348 BIS. (Circunstancias agravantes).- Serán circunstancias agravantes especiales del delito de fraude informático:

A) El parentesco y la vinculación laboral o afectiva con la víctima o el tercero perjudicado.

B) Que el hecho se efectúe en perjuicio del Estado, de cualquier ente público o afectando infraestructuras críticas.

C) Que el hecho se efectúe generando en la víctima el temor de un peligro imaginario o la persuasión de obedecer a una orden de la autoridad".

Artículo 4º.- Agrégase al artículo 34 de la Ley Nº 19.574, de 20 de diciembre de 2017, el siguiente numeral:

"34) Fraude informático cuyo monto real o estimado sea superior a 200.000 UI (doscientas mil unidades indexadas)".

Artículo 5º.- Agréganse al Capítulo VI del Libro II del Título XIII del Código Penal, los siguientes artículos:

"ARTÍCULO 358 QUATER. (Daño informático).- El que por cualquier medio y sin autorización destruya, altere o inutilice datos o sistemas informáticos con la finalidad de causar un daño será castigado con seis a veinticuatro meses de prisión".

"ARTÍCULO 359 TER.- Serán circunstancias agravantes especiales del delito de daño informático:

A) Que el daño ocasionado sea irreparable o fuere imposible retornar a su estado anterior.

B) Que el daño se cometa en perjuicio de documentos electrónicos o sistemas informáticos de carácter estatal o vinculados a infraestructuras críticas".

Artículo 6º.- Agréganse al Capítulo III del Libro II del Título XI del Código Penal, los siguientes artículos:

"ARTÍCULO 297 BIS. (Acceso ilícito a datos informáticos).- El que mediante medios informáticos o telemáticos, sin autorización y sin justa causa acceda, interfiera, difunda, venda o ceda información ajena contenida en soporte digital, será castigado con seis a veinticuatro meses de prisión".

"ARTÍCULO 297 TER. (Interceptación ilícita).- El que sin autorización y sin justa causa intercepte, interrumpa o interfiera por medios técnicos, datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, sean originadas en un sistema informático o efectuadas dentro del mismo, incluyendo las emisiones electromagnéticas provenientes de un sistema informático que transporte los mismos, será castigado con seis a veinticuatro meses de prisión".

"ARTÍCULO 297 QUATER. (Vulneración de datos).- El que mediante la utilización de cualquier medio telemático acceda, se apodere, utilice, o modifique datos confidenciales de terceros, registrados en soportes digitales, o cualquier otro tipo de archivo o registro público o privado, sin autorización de su titular, será castigado con seis a veinticuatro meses de prisión.

El que, habiendo formado parte o no de su descubrimiento, difunda, revele o ceda a terceras personas los datos, hechos o imágenes registrados en soportes digitales será castigado con un año de prisión a cuatro años de penitenciaría.

Constituye circunstancia agravante especial de este delito:

A) Que sea cometido por personas encargadas de custodiar los soportes informáticos, electrónicos, registros o archivos digitales.

B) Que el sujeto pasivo sea un menor de edad o un adulto declarado judicialmente incapaz.

C) Que se cometa con una finalidad lucrativa.

D) Que sea cometido en afectación de datos personales tutelados por la Ley Nº 18.331, de 11 de agosto de 2008.

E) Que se trate de datos estatales o vinculados a infraestructuras críticas".

Artículo 7.- Agréganse al Capítulo III del Título XIII del Libro II del Código Penal, los siguientes artículos:

"ARTÍCULO 347 TER. (Suplantación de identidad).- El 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, será castigado con un año de prisión a seis años de penitenciaría. No constituirá suplantación de identidad la creación de nuevos perfiles destinados exclusivamente a la parodia".

"ARTÍCULO 348 TER. (Circunstancias agravantes especiales).- Serán circunstancias agravantes especiales del delito de suplantación de identidad:

A) Que se cometa con la finalidad de divulgar la información a la cual se accedió.

B) Que se modifiquen, supriman o adulteren datos de la víctima o utilicen las credenciales para vincularse con terceras personas físicas o jurídicas.

C) Que se adquieran, mediante el uso indebido de sus datos personales productos o mercaderías, o contraten servicios a través de medios telemáticos, en nombre de la víctima.

D) Que se suplante la identidad de un organismo estatal u otro vinculado a infraestructuras críticas.

E) La concurrencia con extorsión a la víctima, sus familiares o terceras personas vinculadas, para la obtención de activos o cualquier prestación en especie a los efectos de recuperar las referidas credenciales".

Artículo 8º.- Agrégase al Capítulo VI del Título XIII del Libro II del Código Penal, el siguiente artículo:

"Artículo 358 QUINQUIES. (Abuso de los dispositivos).- El que de forma ilegítima, produzca, adquiera, importe, comercialice o facilite a terceros, programas, sistemas informáticos o telemáticos de cualquier índole, credenciales o contraseñas de acceso a datos informáticos o sistemas de información, destinados inequívocamente a la comisión de un delito, será castigado con seis a veinticuatro meses de prisión".

CAPÍTULO II

MEDIDAS EDUCATIVAS

Artículo 9º. (Campaña nacional educativa).- El Poder Ejecutivo promoverá una campaña nacional educativa sobre el manejo de finanzas personales y ciberseguridad en los centros educativos dependientes de la Dirección General de Educación Secundaria y

de la Dirección General de Educación Técnico-Profesional de la Administración Nacional de Educación Pública, que deberá comprender, además, a beneficiarios de prestaciones servidas por el Banco de Previsión Social, Ceibal y los programas del Instituto Nacional de Empleo y Formación Profesional.

Los conceptos a desarrollar deberán revisarse y actualizarse periódicamente acompasando los avances tecnológicos y serán los siguientes:

A) Medios de pago, (dinero electrónico, diferencia entre subtipos de tarjetas, realización de operaciones en línea y cualquier otro medio de pago electrónico que pudiere desarrollarse).

B) Cuentas bancarias: cajas de ahorro, cuentas corrientes, (diferencias entre ambas y vinculación a la Ley N° 19.210, de 29 de abril de 2014, y al Decreto-Ley N° 14.701, de 12 de setiembre de 1977).

C) Acceso al financiamiento: préstamos (análisis de tasas de interés, plazos, cálculo de cuota contra ingresos mensuales, consecuencias de incumplimientos).

D) Instituciones financieras: diferencia entre agentes clásicos y nuevos participantes, (plataformas de comercio electrónico y mensajería instantánea, entre otras).

E) Planificación presupuestaria: relación ahorro y consumo, costo del dinero.

F) Antecedentes crediticios: clearing de informes, central de riesgos del Banco Central del Uruguay, implicancias e impacto en acceso al crédito.

G) Intangibilidad del salario (límite para el endeudamiento, pago de prestaciones alimenticias, orden de deducciones).

H) Mecanismos de defensa al usuario financiero.

I) Canales digitales y riesgos derivados de su uso inadecuado.

J) Ejercicio de derechos en el entorno digital y aplicación de conceptos de autorregulación, comportamiento ético y empático en el ciberespacio.

K) Fraudes tendientes al acceso de datos personales y financieros, que se determinan según las siguientes definiciones:

1) Phishing: suplantación de identidad, técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esas personas.

2) Vishing: tipo de estafa de ingeniería social por teléfono en la que a través de una llamada, se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima.

3) Smishing: técnica que consiste en el envío de un mensaje de texto por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública u otros) con el objetivo de robarle información privada o causarle un perjuicio económico.

4) Malware: hace referencia al software malicioso, que afecte los intereses del usuario, entendiéndose software al conjunto de programas y rutinas que permiten a una computadora realizar determinadas tareas.

5) Troyano: es un programa que instala otros programas a menudo malware, sin consentimento.

6) Ingeniería social: son las diferentes técnicas de manipulación que usan los ciberdelincuentes para obtener información confidencial de los usuarios, engañando a sus víctimas haciéndose pasar por otra persona.

L) Buenas prácticas para el uso de canales digitales (riesgos asociados a su utilización por parte de menores de edad, relevancia de la supervisión).

Asimismo, deberá asegurarse la igualdad en el acceso a las tecnologías de la información y de la comunicación, así como la equidad de género en su uso y acceso por lo que las entidades competentes deberán desarrollar campañas de seguridad digital en

todo el territorio nacional con el fin de generar espacios de formación, capacitación, sociabilización y accesibilidad en las tecnologías de la información y la educación de forma equitativa a hombres y mujeres e igualitaria en materia de generaciones y discapacidad.

CAPÍTULO III

REGISTRO DE CIBERDELINCUENTES

Artículo 10. (Registro de antecedentes).- Facúltase 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, operativas fraudulentas y tomar medidas preventivas conjuntas sobre los beneficiarios de éstas.

A los solos efectos de compartir entre sí la información a que refiere el inciso anterior, no aplicarán a las instituciones y entidades mencionadas las limitaciones impuestas por el Decreto-Ley N° 15.322, de 17 de setiembre de 1982, quedando dichas instituciones y entidades facultadas para compartir sus registros con las autoridades jurisdiccionales, a los efectos de radicar denuncias y realizar gestiones tendientes a prevenir y mitigar los ciberdelitos tipificados en la presente ley.

CAPÍTULO IV

PREVENCIÓN DE TRANSACCIONES NO CONSENTIDAS

Artículo 11. (Inmovilización de fondos).- Facúltase a las instituciones de intermediación financiera y a las entidades emisoras de dinero electrónico a la no ejecución de cualquier tipo de orden de retiro o transferencia de activos brindada por personas físicas o jurídicas titulares o apoderados de cuentas, cuando hubieren tomado conocimiento, por cualquier medio de comunicación fehaciente, que en las cuentas referidas ingresaron fondos de terceros a través de transacciones que les fueran declaradas como desconocidas y no autorizadas por el titular de las cuentas de origen de los fondos transferidos. Lo dispuesto comprende instrucciones efectuadas directamente por los titulares de la cuenta así como instrucciones impartidas por sus representantes o apoderados a cualquier título.

La inmovilización de fondos referida en el inciso anterior se aplicará a las cuentas correspondientes y comprenderá los saldos actuales e ingresos futuros de fondos o valores a dichas cuentas. En cualquier caso, la inmovilización de fondos alcanzará hasta el límite del monto de las transacciones denunciadas como desconocidas y no autorizadas por el titular de las cuentas de origen de los fondos transferidos, debiendo las instituciones de intermediación financiera y las entidades emisoras de dinero electrónico ejecutar toda orden que excediera dicho límite, salvo que las mismas no cumplan con requisitos legales o contractuales.

La inmovilización de los fondos consecuentemente con lo dispuesto en los incisos anteriores, deberá ser comunicada dentro del plazo de un día hábil al Banco Central del Uruguay (BCU), quien podrá solicitar información adicional a las instituciones de intermediación financiera y a las entidades emisoras de dinero electrónico donde se encuentran radicadas las cuentas de origen y destino vinculadas a las transacciones denunciadas como desconocidas y no autorizadas y, previo análisis de la información a la que acceda, podrá instruir dejar sin efecto la inmovilización de fondos.

La inmovilización de fondos deberá dejarse sin efecto y comunicarse al BCU cuando ocurra alguna de las siguientes situaciones:

A) La institución de intermediación financiera o la entidad emisora de dinero electrónico donde se encuentra radicada la cuenta afectada no hubiere recibido dentro del plazo de cuarenta y ocho horas de efectuada la inmovilización, constancia de denuncia presentada por el titular de la cuenta origen de los fondos ante autoridad competente (Ministerio del Interior o Fiscalía General de la Nación).

B) La institución de intermediación financiera o la entidad emisora de dinero electrónico donde se encuentra radicada la cuenta afectada no hubiere recibido, dentro del plazo de treinta días siguientes a la recepción de la constancia de denuncia referida en el literal A), una orden jurisdiccional confirmando la medida de inmovilización.

C) La institución de intermediación financiera o la entidad emisora de dinero electrónico donde se encuentra radicada la cuenta afectada por inmovilización recibiera de cualquier autoridad jurisdiccional competente instrucción de dejar sin efecto la inmovilización referida.

D) La institución de intermediación financiera o la entidad emisora de dinero electrónico donde se encuentra radicada la cuenta afectada por inmovilización recibiera, del titular de la misma, elementos de convicción suficiente o documentación fehaciente que, a su exclusivo criterio, indiquen que la transacción denunciada fue efectivamente autorizadas por el titular de la cuenta de origen.

Las instituciones de intermediación financiera y las entidades emisoras de dinero electrónico podrán radicar o ampliar denuncias ante las autoridades competentes, y realizar gestiones interinstitucionales, quedando facultadas para brindar todos los datos vinculados a las operaciones no consentidas.

Sala de Sesiones de la Cámara de Representantes, en Montevideo, a 12 de julio de 2023.

SEBASTIÁN ANDÚJAR
Presidente

FERNANDO RIPOLL FALCONE
Secretario