PARLAMENTO
DEL URUGUAY
CÁMARA DE REPRESENTANTES
Secretaría

COMISIÓN DE CONSTITUCIÓN, CÓDIGOS, LEGISLACIÓN GENERAL Y ADMINISTRACIÓN INTEGRADA CON LA ESPECIAL DE INNOVACIÓN, CIENCIA Y TECNOLOGÍA

ANEXO I AL
REPARTIDO Nº 492
JUNIO DE 2023

CARPETA Nº 1734 DE 2021

TIPIFICACIÓN DE CIBERDELITO

N o r m a s

I n f o r m e s

XLIX Legislatura

Í N D I C E

	Página
Informe en mayoría	1
Proyecto de ley	5
Informe en minoría	12
Proyecto de resolución	13
Disposiciones referidas	17

COMISIÓN DE CONSTITUCIÓN, CÓDIGOS,
LEGISLACIÓN GENERAL Y ADMINISTRACIÓN
INTEGRADA CON LA ESPECIAL DE INNOVACIÓN,
CIENCIA Y TECNOLOGÍA

INFORME EN MAYORÍA

Señores Representantes:

La Comisión de Constitución, Códigos, Legislación General y Administración integrada con la Especial de Innovación, Ciencia y Tecnología ha considerado el proyecto de ley por el que se dictan normas sobre ciberdelitos.

Durante los últimos años, en nuestro país y el mundo la tecnología ha avanzado a pasos agigantados: todos los días aparecen nuevos descubrimientos, programas y sistemas que se van incorporando a las actividades diarias, ya sea con fines laborales, de esparcimiento, de negocios, de compras, como de tantos otros, pero también canalizamos a través de estas herramientas nuestros datos personales, medios de pago (cuentas bancarias, tarjetas de crédito, billeteras digitales y demás), realizamos transferencias, pagos, subimos fotos, videos, estados, todo a través de Internet, mediante el uso de plataformas y aplicaciones que, sin perjuicio de su seguridad, muchas veces son vulneradas o utilizadas para cometer hechos ilícitos.

Estamos más conectados digitalmente que nunca y los delincuentes se están aprovechando de esta transformación en línea para atacar redes, infraestructuras y sistemas informáticos. Esto tiene una enorme repercusión económica y social tanto para el gobierno como para las personas físicas, jurídicas e incluso los Estados.

El presente proyecto de ley pretende atender una problemática relevante y cada vez más recurrente, tanto en nuestro país como en el mundo: la ciberdelincuencia.

Hablamos de una realidad muy dinámica, la cual se debe atender y seguir muy de cerca pero que indudablemente requiere la existencia de normativa específica, que permita una mayor persecución y control de las actividades fraudulentas que se suscitan frecuentemente a través de los distintos medios informáticos.

De este modo, en atención a la realidad digital que nos rodea, se torna imperiosa y urgente la necesidad de crear un marco legal regulatorio específico para enfrentar la llamada ciberdelincuencia, esas conductas que lesionan gravemente determinados bienes jurídicos.

Sin perjuicio de que se requiere un abordaje integral por parte de todos los actores (jueces, fiscales, policía, academia, empresas públicas y privadas, sociedad en general) resulta indispensable contar con un marco regulatorio, medidas educativas y mecanismos de protección, por lo cual se ha entendido que este es el primer paso dentro de un largo camino que debe transitar el Uruguay.

Lo que se quiere es lograr proteger a los usuarios, quienes permanentemente son víctimas de actividades fraudulentas. Desde nuestro lugar,

debemos actualizar y reformar la regulación para atender este fenómeno, que implica modificaciones adecuadas y reales que supongan una mayor protección para la sociedad en su conjunto y de cierto modo, constituyan un freno a esta actividad delictiva que configura un flagelo constante para ciudadanos de todas las edades.

Los ciberataques no son algo novedoso; ocurren y han ocurrido tanto en nuestro país como en el mundo, convirtiéndose muchas veces en delitos transnacionales, lo que dificulta aun más su combate y persecución. En este sentido hemos observado que se ha tornado una situación preocupante e insostenible, que requiere una rápida acción de todos los actores, pero principalmente desde los órganos legislativos que integramos.

El referido avance de la ciberdelincuencia en Uruguay ha dejado de manifiesto las vulnerabilidades de nuestro sistema: tanto la carencia de regulación específica como de educación sobre ciberseguridad y demás herramientas, que permitan mitigar el impacto del accionar de los delincuentes.

Es por ello que el objetivo principal del presente proyecto es plasmar distintas alternativas tendientes a regular y fortalecer las debilidades de nuestro actual régimen penal, teniendo en cuenta que los ciberataques son una realidad y llegaron para quedarse, que serán cada vez más habituales y a mayor escala, capaces de perjudicar a un gran número de usuarios, reflejando la mutación de los patrones delictivos que conocíamos previamente y trasladando su ámbito común de acción como lo pueden ser la vía pública o las actividades privadas de los individuos, hacia el ciberespacio. De esta forma, contestes con el fenómeno de la globalización, la transformación de los medios masivos de comunicación, la modificación en la forma de comunicarnos en sociedad; todo lo cual se vio fuertemente agravado por los efectos colaterales de la pandemia que el mundo atravesó desde marzo del año 2020, que no hizo más que acrecentar nuestra actividad cibernética, generó cambios en materia laboral (teletrabajo), la educación se tornó forzosamente virtual, las relaciones humanas pasaron a desarrollarse enteramente de forma remota a través de distintas aplicaciones de mensajería y videollamadas. Por consiguiente toda esa migración hacia la virtualidad y el incremento del uso de la tecnología indefectiblemente supuso y supone una mayor exposición a los ciberataques. Constantemente somos protagonistas de intercambios virtuales sin conocer ni tener formación alguna en referencia a los riesgos que ello apareja.

Tales fueron los avances tecnológicos en los últimos años, que comenzamos a utilizar tímidamente los correos electrónicos; luego tuvimos la posibilidad de enviar mensajes de texto por plataformas de mensajería instantánea, pudiendo conectarnos al instante con cualquier persona en cualquier lugar del mundo; el surgimiento de las redes sociales nos permitió subir al instante fotos y estados que no son otra cosa que el reflejo de nuestras actividades diarias; y habitualmente transaccionamos libremente por el mundo, pudiendo acceder a distintos medios de pago, a través de canales digitales, siendo este punto uno de los pilares fundamentales que el presente proyecto busca regular, brindando más y mejor protección para los usuarios de dichos sistemas.

Ante este contexto, donde gran parte de nuestras actividades se desarrollan desde la virtualidad, consideramos necesario crear medidas regulatorias para evitar y mitigar el riesgo de que la tecnología, las redes informáticas, así como toda la información electrónica que compartimos mediante éstas se utilicen para la comisión de las distintas conductas reprochables, que perjudican directamente tanto a las personas físicas como jurídicas que interactúan en Internet, como así también al Estado, que se encuentra imposibilitado de sancionar a los autores de las actividades delictivas y fraudulentas, pues no existen aún en nuestro ordenamiento jurídico tipos penales para perseguir y condenar

la ciberdelincuencia. En el mismo sentido, resulta indispensable recordar que Uruguay tampoco ha adherido a convenios internacionales relativos a la materia que nos compete.

Mediante el presente proyecto se pretende establecer los distintos tipos penales internacionalmente consagrados, siempre garantizando el justo equilibrio entre la acción penal a cargo del Estado y los legítimos intereses de la sociedad respecto a los derechos fundamentales; en pro de contar con una regulación efectiva y garantista.

Nuestro país, a diferencia de otros países de la región y del mundo, no ha abordado el tema de la tipificación de los distintos delitos informáticos establecidos en el Convenio de Budapest, de 23 de noviembre del año 2001, por el Consejo de Europa; ni sus Protocolos adicionales. Debemos destacarse que es éste, el Tratado Internacional sobre la Ciberdelincuencia, el que brinda herramientas no solo para proteger a los ciudadanos contra los delitos cometidos en Internet, sino también para generar legislación procesal, brindando nociones para el manejo de la evidencia digital, así como para lograr la cooperación internacional en la materia. Esta cooperación internacional resulta muy necesaria en la actualidad, atendiendo como mencionamos previamente, al carácter transnacional de los ciberdelitos.

Sin perjuicio de que en nuestro ordenamiento jurídico existen actualmente ciertas normas desperdigadas en distintos cuerpos normativos, la carencia de sistematización y de una regulación concreta y en buen romance se traduce en que algunas maniobras delictivas acaben tipificadas como estafas o eventualmente receptación, cuando podrían encuadrarse en otros tipos penales que hoy no se recogen en nuestro ordenamiento.

Es necesario por lo tanto que Uruguay regule en esta materia con el fin de delimitar y proteger la actuación de los usuarios digitales, garantizando derechos y obligaciones al momento de explorar el ciberespacio.

En cuanto al trámite parlamentario del presente proyecto de ley, se han mantenido reuniones dentro y fuera de la Comisión Especial de Innovación, Ciencia y Tecnología, a los efectos de conocer las necesidades y opiniones de los distintos intervinientes. Posteriormente se continuó analizando en la Comisión de Constitución, Códigos, Legislación General y Administración integrada con la Especial de Innovación, Ciencia y Tecnología, bajo el entendido de que las nuevas normas implican modificar el Código Penal vigente.

Las modificaciones aparejan también la inclusión de otros puntos, tales como la ampliación de contenidos para la campaña nacional educativa, la generación de un Registro de Ciberdelincuentes y el Proceso de Prevención de Transacciones no consentidas, entre otras.

Como corolario de todo lo antedicho, habiendo sido presentado el 22 de julio de 2021, recibido aportes de los Ministerios del Interior, de Educación y Cultura, de Relaciones Exteriores, de la Fiscalía General de la Nación, de la Facultad de Derecho, del Banco Central del Uruguay, del Banco de la República Oriental del Uruguay, de la Asociación de Bancos Privados del Uruguay, de la Cámara Uruguaya de las Tecnologías de la Información y votado por mayoría el 14 de junio de 2023 en la Comisión de Constitución, Códigos, Legislación General y Administración integrada con la Especial de Innovación, Ciencia y Tecnología, es que entendemos indispensable la aprobación de este proyecto, que va a permitir el fortalecimiento de las vulnerabilidades descriptas sobre una problemática que ha sido abarcada por la mayoría de países del mundo y regulada en el derecho comparado, situación que implica un gran desafío a futuro para nuestro país. Se ha tornado imperioso contar con regulación expresa y sistematizada en el

ordenamiento jurídico nacional así como generar programas educativos relativos a ciberseguridad y educación financiera. Finalmente, se ha entendido que este proyecto de ley constituye la base para avanzar en la aprobación del Convenio de Budapest, sobre el cual el Estado uruguayo ha manifestado voluntad de ser Estado parte y ha recibido una delegación del Consejo de Europa, la cual le ha dado su visto bueno.

Por las razones expuestas, esta Comisión, en mayoría, aconseja al Cuerpo la aprobación del proyecto de ley que se acompaña.

Sala de la Comisión, 14 de junio de 2023

SEBASTIÁN CAL
MIEMBRO INFORMANTE
FERNANDA ARAÚJO
MARIO COLMAN
DIEGO ECHEVERRÍA
MARTÍN ELGUE
RODRIGO GOÑI REYES
MARTÍN MELAZZI
OPE PASQUET
CARLOS TESTA

PROYECTO DE LEY

CAPÍTULO I

TIPIFICACIÓN DE CIBERDELITOS

Artículo 1°.- 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 2°.- 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 13 años de edad, con discapacidad, deficiencias físicas o psíquicas".

Artículo 3°.- 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 4°.- 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 5°.- 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 6°.- 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 8°.- 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 9°. (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 (BPS), Ceibal y los programas del Instituto Nacional de Empleo y Formación Profesional (INEFOP).

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 Ley Nº 19.210, de 29 de abril de 2014, y al Decreto-Ley NC 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 (BCU), 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 consentimiento;

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 Nº 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 la Comisión, 14 de junio de 2023

SEBASTIÁN CAL
MIEMBRO INFORMANTE
FERNANDA ARAÚJO
MARIO COLMAN
DIEGO ECHEVERRÍA
MARTÍN ELGUE
RODRIGO GOÑI REYES
MARTÍN MELAZZI
OPE PASQUET
CARLOS TESTA

_____

INFORME EN MINORÍA

Señores Representantes:

Votamos negativamente este proyecto, por múltiples razones, entre las que se cuentan la omisión de un abordaje integral del problema de la seguridad digital, en la que están las víctimas de los delitos y sus victimarios, pero también las entidades financieras y no financieras y el Estado que es en definitiva, el que debe regular los estándares de protección de los derechos de los hombres y mujeres que viven en nuestro país.

No viene a solucionar los propósitos originales que están en su exposición de motivos. No contempla reparación a las víctimas ni mecanismos para enmendar errores que los usuarios de métodos digitales de pago puedan cometer. Es inflacionista penal y no es preciso con la tipificación de delitos, con las consecuencias negativas que esto trae, al incluir conductas inocuas o cotidianas dentro de los posibles comportamientos a censurar. Finalmente es deficiente a nivel de técnica legislativa y ha recibido las críticas de la academia y de operadores judiciales, las cuales han sido mayoritariamente ignoradas.

En el debate en Cámara detallaremos lo anteriormente expuesto.

Por las razones expuestas esta Comisión, en minoría, aconseja al Cuerpo la aprobación del proyecto de resolución que se acompaña.

Sala de la Comisión, 14 de junio de 2023

LILIÁN GALÁN
MIEMBRO INFORMANTE
CECILIA BOTTINO FIURI
LUIS GALLO CANTERA
CLAUDIA HUGO
ENZO MALÁN CASTRO
NICOLÁS MESA WALLER
GUSTAVO OLMOS
MARIANO TUCCI MONTES DE OCA

PROYECTO DE RESOLUCIÓN

Recházase el proyecto de ley caratulado “Tipificación de ciberdelito. Normas”, contenido en la Carpeta 1734/2021.

Sala de la Comisión, 14 de junio de 2023

LILIÁN GALÁN
MIEMBRO INFORMANTE
CECILIA BOTTINO FIURI
LUIS GALLO CANTERA
CLAUDIA HUGO
ENZO MALÁN CASTRO
NICOLÁS MESA WALLER
GUSTAVO OLMOS
MARIANO TUCCI MONTES DE OCA

A P É N D I C E

Disposiciones referidas

LEY Nº 19.574, DE 20 DE DICIEMBRE DE 2017

___

CAPÍTULO V 4°
DE LOS DELITOS DE LAVADO DE ACTIVOS

Artículo 34 (Actividades delictivas precedentes).- Son actividades delictivas precedentes del delito de lavado de activos en sus diversas modalidades previstas en los artículos 30 a 33 de la presente ley, los siguientes delitos:

1) Los delitos previstos en el Decreto-Ley N° 14.294, de 31 de octubre de 1974 en las redacciones dadas por la Ley N° 17.016, de 22 de octubre de 1998 y Ley N° 19.172, de 20 de diciembre de 2013 (narcotráfico y delitos conexos).
2) Crímenes de genocidio, crímenes de guerra y de lesa humanidad tipificados por la Ley N° 18.026, de 25 de setiembre de 2006.
3) Terrorismo.
4) Financiación del terrorismo.
5) Contrabando cuyo monto real o estimado sea superior a 200.000 UI (doscientas mil unidades indexadas).
6) Tráfico ilícito de armas, explosivos, municiones o material destinado a su producción.
7) Tráfico ilícito de órganos, tejidos y medicamentos.
8) Tráfico ilícito y trata de personas.
9) Extorsión.
10) Secuestro.
11) Proxenetismo.
12) Tráfico ilícito de sustancias nucleares.
13) Tráfico ilícito de obras de arte, animales o materiales tóxicos.
14) Estafa cuyo monto real o estimado sea superior a 200.000 UI (doscientas mil unidades indexadas).
15) Apropiación indebida cuyo monto real o estimado sea superior a 200.000 UI (doscientas mil unidades indexadas).
16) Los delitos contra la Administración Pública incluidos en el Título IV del Libro II del Código Penal y los establecidos en la Ley N° 17.060, de 23 de diciembre de 1998 (delitos de corrupción pública).
17) Quiebra fraudulenta.
18) Insolvencia fraudulenta.
19) El delito previsto en el artículo 5° de la Ley N° 14.095, de 17 de noviembre de 1972 (insolvencia societaria fraudulenta).
20) Los delitos previstos en la Ley N° 17.011, de 25 de setiembre de 1998 y sus modificativas (delitos marcarios).
21) Los delitos previstos en la Ley N° 17.616, de 10 de enero de 2003 y sus modificativas (delitos contra la propiedad intelectual).
22) Las conductas delictivas previstas en la Ley N° 17.815, de 6 de setiembre de 2004, en los artículos 77 a 81 de la Ley N° 18.250, de 6 de enero de 2008 y todas aquellas conductas ilícitas previstas en el Protocolo Facultativo de la Convención de los Derechos del Niño sobre venta, prostitución infantil y utilización en pornografía o que refieren a trata, tráfico o explotación sexual de personas.
23) La falsificación y la alteración de moneda previstas en los artículos 227 y 228 del Código Penal.
24) Fraude concursal, según lo previsto en el artículo 248 de la Ley N° 18.387, de 23 de octubre de 2008.
25) Defraudación tributaria, según lo previsto en el artículo 110 del Código Tributario, cuando el monto de el o los tributos defraudados en cualquier ejercicio fiscal sea superior a:
    A) 2.500.000 UI (dos millones quinientos mil unidades indexadas) para los ejercicios iniciados a partir del 1° de enero de 2018.
    B) 1.000.000 UI (un millón de unidades indexadas) para los ejercicios

iniciados a partir del 1° de enero de 2019.

Dicho monto no será exigible en los casos de utilización total o parcial de facturas o cualquier otro documento, ideológica o materialmente falsos con la finalidad de disminuir el monto imponible u obtener devoluciones indebidas de impuestos.

En las situaciones previstas en el presente numeral el delito de defraudación tributaria podrá perseguirse de oficio.

26) Defraudación aduanera, según lo previsto en el artículo 262 del Código Aduanero, cuando el monto defraudado sea superior a 200.000 UI (doscientas mil unidades indexadas).

En este caso el delito de defraudación aduanera podrá perseguirse de oficio.

27) Homicidio cometido de acuerdo a lo previsto por el artículo 312 numeral 2 del Código Penal.

28) Los delitos de lesiones graves y gravísimas previstos en los artículos 317 y 318 del Código Penal, cometidos de acuerdo a lo previsto en el artículo 312 numeral 2 del Código Penal.

29) Hurto, según lo previsto en el artículo 340 del Código Penal, cuando sea cometido por un grupo delictivo organizado y cuyo monto real o estimado sea superior a 100.000 UI (cien mil unidades indexadas).

30) Rapiña, según lo previsto en el artículo 344 del Código Penal, cuando sea cometida por un grupo delictivo organizado y cuyo monto real o estimado sea superior 100.000 UI (cien mil unidades indexadas).

31) Copamiento, según lo previsto en el artículo 344 bis del Código Penal, cuando sea cometido por un grupo delictivo organizado y cuyo monto real o estimado sea superior a 100.000 UI (cien mil unidades indexadas).

32) Abigeato, según lo previsto en el artículo 258 del Código Rural, cuando sea cometido por un grupo delictivo organizado y cuyo monto real o estimado sea superior a 100.000 UI (cien mil unidades indexadas).

Se entiende por grupo delictivo organizado, un conjunto estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer dichos delitos, con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material.

33) Asociación para delinquir, según lo previsto en el artículo 150 del Código Penal.

A efectos del intercambio de información entre Estados, tanto por la vía de la cooperación jurídica penal como de la cooperación administrativa entre Unidades de Inteligencia Financiera, no regirán los umbrales establecidos en los numerales anteriores.

———————

LEY Nº 19.210, DE 29 DE ABRIL DE 2014

———

TÍTULO I DE LOS MEDIOS DE PAGO ELECTRÓNICOS CAPÍTULO ÚNICO 9°

Artículo 1°.- (Medio de pago electrónico).- Se entenderá por medio de pago electrónico las tarjetas de débito, las tarjetas de crédito, los instrumentos de dinero electrónico y las transferencias electrónicas de fondos, así como todo otro instrumento análogo que permita efectuar pagos electrónicos a través de cajeros automáticos, por Internet o por otras vías, de acuerdo a lo que establezca la reglamentación.

Los pagos efectuados a través de medios de pago electrónicos tienen pleno efecto cancelatorio sobre las obligaciones en cumplimiento de las cuales se efectúan. En el caso de las transferencias electrónicas de fondos, el pleno efecto cancelatorio se producirá al momento de la acreditación del monto transferido en la cuenta de destino.

DECRETO-LEY N° 14.701, DE 12 DE SETIEMBRE DE 1977

TITULO PRIMERO - DE LOS TITULOS-VALORES EN GENERAL 9°

CAPITULO I - DISPOSICIONES GENERALES

SECCION I – GENERALIDADES

Artículo 1°.- Los títulos-valores son los documentos necesarios para ejercitar el derecho literal y autónomo que en ellos se consigna.

DECRETO LEY Nº 15.322, DE 17 DE SETIEMBRE DE 1982

Artículo 1°.- Toda persona pública no estatal o privada que realice intermediación financiera quedará sujeta a las disposiciones de esta ley, a los reglamentos y a las normas generales e instrucciones particulares, que dicte el Banco Central del Uruguay para su ejecución. 10

A los efectos de esta ley, se considera intermediación financiera la realización habitual y profesional de operaciones de intermediación o mediación entre la oferta y la demanda de títulos valores, dinero o metales preciosos.