REPÚBLICA ORIENTAL DEL URUGUAY

Cámara de Representantes
Secretaría

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

REPARTIDO Nº 849
ABRIL DE 2023

CARPETA Nº 3473 DE 2023

SEGURIDAD DIGITAL

Regulación

XLIX Legislatura

PROYECTO DE LEY

Artículo 1°. (Finalidad de la ley).- La presente ley tiene como finalidad la protección de la seguridad digital de las personas, para garantizar que las mismas puedan actuar libre y responsablemente en el uso de las tecnologías de la información y la comunicación, minimizando las amenazas a sus derechos fundamentales.

Artículo 2°. (Definiciones).- A los efectos de la presente ley se formulan las siguientes definiciones:

a) Ciberdelito: se entiende por ciberdelito, cualquier forma de conducta ilícita ejecutada en el ámbito de interacción social o que ocasione interacciones entre dispositivos definida por el uso de las tecnologías de la información y la comunicación.

b) Entidad Financiera: se entiende por entidad financiera, las instituciones de intermediación financiera y a las entidades emisoras de instrumentos electrónicos.

CAPÍTULO I

REPARACIÓN DE LAS VÍCTIMAS

Artículo 3°. (Sanción pecuniaria).- En la sentencia de condena por los delitos cometidos mediante el uso de las tecnologías de la información y la comunicación, además de la pena, se dispondrá una reparación patrimonial para la víctima por un monto equivalente a doce ingresos mensuales del condenado, o en su defecto doce salarios mínimos, sin perjuicio de su derecho a seguir la vía procesal correspondiente para obtener la reparación integral del daño.

Artículo 4°. (Destino de la multa).- El importe de las multas impuestas por incumplimiento de las obligaciones de seguridad de los emisores de instrumentos electrónicos corresponderá a la víctima del delito que haya efectuado la denuncia ante la entidad correspondiente. Dicho importe será abonado, siempre y cuando se verifiquen acumulativamente los siguientes requisitos:

a) La entidad financiera haga efectivo su pago.

b) Cuando el acto administrativo que disponga la sanción adquiera el carácter de firme.

CAPÍTULO II

OBLIGACIONES Y RESPONSABILIDADES DE LAS ENTIDADES FINANCIERAS

Artículo 5°. (Notificación y rectificación de transferencias y operaciones de pago no autorizadas o ejecutadas incorrectamente).- La entidad financiera deberá notificar previamente al usuario, de todas las transferencias diarias por un monto igual o mayor a un Salario Mínimo Nacional (SMN), efectuadas en una o varias transacciones.

El usuario podrá solicitar a la entidad bancaria que no se le realice la notificación indicada en el inciso primero.

La entidad financiera deberá ofrecer al usuario, la opción de notificación previa a la realización de una operación u operaciones con cualquier medio de pago por un monto diario igual o mayor a un Salario Mínimo Nacional, efectuada en una o varias transacciones.

El usuario obtendrá la rectificación por parte del proveedor de servicios de pago de una operación no autorizada luego de ser notificado previamente; o ejecutada incorrectamente por responsabilidad de la entidad financiera, si el usuario lo comunica a la entidad en un plazo de diez (10) días hábiles, computado desde el momento en que tenga conocimiento de la transacción de conformidad con la normativa vigente.

Los costos relativos al procedimiento de notificación previa no podrán ser transferidos al usuario.

Artículo 6°. (Inmovilización de fondos).- Autorízase a las entidades financieras a suspender la ejecución de cualquier operación de retiro o transferencia efectuada por personas físicas o jurídicas titulares o apoderados de cuentas, cuando existan sospechas fundadas de operaciones no autorizadas por el titular o apoderado.

Artículo 7°. (Seguro de responsabilidad o garantía equivalente).- Las entidades financieras están obligadas a contratar un seguro para la responsabilidad en la prestación de servicios cuando se produzca un incumplimiento a la normativa relativa a las obligaciones de seguridad del sistema.

En defecto de la contratación del seguro, deberán depositar en el Banco Central del Uruguay en garantía de las obligaciones referidas en la presente ley, el monto que la autoridad monetaria establezca dentro de los treinta (30) días siguientes a la vigencia de la presente ley.

Artículo 8°. (Responsabilidad civil).- Las entidades financieras serán civilmente responsables por los daños sufridos por los usuarios por el incumplimiento de las normas de seguridad previstas en la normativa, por la actuación ajena a la diligencia de la buena persona de negocios y por no ajustarse a los estándares internacionalmente reconocidos en materia de seguridad informática, según la normativa interna y los tratados internacionales ratificados.

Artículo 9°. (Responsabilidad administrativa).- Las empresas financieras que no adopten las medidas de seguridad del sistema previstas en la normativa serán sancionadas por el Banco Central del Uruguay con una multa no inferior a 1/1000 (uno por mil) ni superior a 2/1000 (dos por mil) de la responsabilidad básica establecida para entidades financieras.

Las empresas financieras que no adopten las medidas de seguridad del sistema previstas en la normativa, causando daños a sus clientes, usuarios o terceros, serán sancionadas por el Banco Central del Uruguay con una multa no inferior a 2/1000 (dos por mil) ni superior a 3/1000 (tres por mil) de la responsabilidad básica establecida para entidades financieras.

CAPÍTULO III

INVESTIGACIÓN ACADÉMICA Y ACCIONES DE IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD

Artículo 10.- Se entenderá que cuenta con autorización para el acceso a un sistema informático, el o la que en el marco de investigaciones académicas, investigaciones de

vulnerabilidad o para mejorar la seguridad informática, acceda a un sistema informático, si la conducta no tiene finalidades lucrativas.

Las personas físicas o jurídicas tienen el derecho a la disponibilidad de los dispositivos propios, por lo que el propietario de un dispositivo electrónico tendrá derecho a alterar su software o hardware para repararlo, evitar la obsolescencia programada, así como para cualquier otra modificación siempre que las mismas sean sin fines de lucro, por lo que no incurrirán en responsabilidad civil, penal ni administrativa.

Dicho derecho se extiende a la persona que el propietario del dispositivo encargue su reparación o modificación; así como a quien adquiera o enajene herramientas necesarias para la reparación o modificación de los dispositivos.

CAPÍTULO IV

DISPOSICIONES FORMATIVAS Y EDUCATIVAS

Artículo 11. (Formación y educación en seguridad digital).- Deberá promoverse la formación y educación en seguridad digital, con la finalidad de brindar las herramientas para garantizar la seguridad digital de las personas y desarrollar políticas educativas para informar y capacitar en el uso de tecnologías de la información y la comunicación, tanto en el sistema educativo, en la formación profesional como a beneficiarios del Banco de Previsión Social y de las otras entidades previsionales.

Artículo 12. (Equidad en el acceso y seguridad digital).- 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 V

DISPOSICIONES PENALES

Artículo 13.- Incorpórase al artículo 288 del Código Penal el siguiente inciso:

"La misma pena se aplicará si la violencia o amenaza se ejerciere mediante tecnologías de la información o de la comunicación".

Artículo 14.- Incorpórase al Código Penal la siguiente disposición:

"301 bis. (Acceso a información en soporte digital).- El o la que por medios fraudulentos, sin autorización y sin justa causa acceda, interfiera, difunda, venda o ceda información ajena contenida en soporte digital, será castigado con una pena de seis a veinticuatro meses de prisión".

Artículo 15.- Incorpórase al Código Penal la siguiente disposición:

"348 bis. (Estafa digital).- El o la que con estratagemas o engaños artificiosos, indujeron en error a alguna persona a los efectos de obtener información necesaria, 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, será castigado con seis meses de prisión a cuatro años de penitenciaría".

Artículo 16.- Incorpórase al Código Penal la siguiente disposición:

"358 quater. (Daño informático).- El o la 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 una pena de tres a quince meses de prisión".

Artículo 17. (Agravante por el uso de tecnologías de la información y la comunicación).- Se considerará como agravante la comisión del delito mediante el uso de tecnologías de la información y la comunicación si con ello se acredita la existencia de una alta dañosidad del bien jurídico protegido o si por ese medio se ha alcanzado a una mayor cantidad de víctimas.

Artículo 18. (Responsabilidad por no cumplimiento de normas de seguridad digital).- El o la titular de la entidad financiera, o en su caso, quien ejerciendo efectivamente en su nombre el poder de dirección en la misma, no adoptare las medidas de seguridad del sistema previstas en la normativa, de forma que pongan en peligro grave y concreto el patrimonio o los datos personales del cliente, será castigado con tres a veinticuatro meses de prisión.

Artículo 19. (Exención de responsabilidad).- Estará exento de responsabilidad el o la que por medio de las tecnologías de la información y comunicación:

A) obtuviese o difundiere cualquier clase de manifestación sobre asuntos de interés público, referida tanto a funcionarios públicos como a personas que, por su profesión u oficio, tengan una exposición social de relevancia, o a toda persona que se haya involucrado voluntariamente en asuntos de interés público.

B) reprodujere cualquier clase de manifestación sobre asuntos de interés público, cuando el autor de las mismas se encuentre identificado.

C) efectuase o difundiere cualquier clase de manifestación humorística o artística, y toda otra expresión amparada por el derecho a la libertad de expresión, efectuada sin real malicia.

CAPÍTULO VI

OTRAS DISPOSICIONES

Artículo 20. (Derechos del consumidor).- Modifícase el artículo 6º literal c) de la "Ley de relaciones de consumo. Defensa del Consumidor" Nº 17.250, de 11 de agosto de 2000, por la siguiente redacción:

"La información suficiente, clara, veraz, en idioma español sin perjuicio que puedan emplearse además otros idiomas, incluyendo la documentación técnica sobre los componentes físicos y de software que permita una correcta reparación o modificación sobre los dispositivos electrónicos".

Artículo 21. (Datos personales).- Agréguese al artículo 1º de la "Ley de Protección de datos personales" Nº 18.331, de 11 de agosto de 2008, el inciso segundo:

"Se considerarán datos personales los que se encuentren contenidos en cualquier soporte físico o digital".

Artículo 22. (Potestades sancionatorias).- Sustitúyese el artículo 35 de la Ley Nº 18.331, de 11 de agosto de 2008, en la redacción dada por el artículo 83 de la Ley Nº 19.355, de 29 de diciembre de 2015, por el siguiente:

"ARTÍCULO 35.- El órgano de control podrá aplicar las siguientes sanciones a los responsables de las bases de datos, encargados de tratamiento de datos personales y demás sujetos alcanzados por el régimen legal, en caso de que se violen las normas de la presente ley, las que se graduarán en atención a la gravedad, reiteración o reincidencia de la infracción cometida:

1) Observación.

2) Apercibimiento.

3) Multa de hasta 500.000 UI (quinientas mil unidades indexadas).

4) Suspensión de la base de datos respectiva por el plazo de cinco días.

5) Clausura de la base de datos respectiva. A tal efecto se podrá promover ante los órganos jurisdiccionales competentes la clausura de las bases de datos que se comprobare infringieren o transgredieren la presente ley.

Los hechos constitutivos de la infracción serán documentados de acuerdo a las formalidades legales. La clausura deberá decretarse dentro de los tres días siguientes a aquel en que la hubiere solicitado la Unidad Reguladora y Control de Datos Personales, la cuál quedará habilitada a disponerla por sí en caso de que el Juez no se pronunciare dentro de dicho término.

En este último caso, si el Juez denegare posteriormente la clausura, esta deberá levantarse de inmediato por la Unidad Reguladora y Control de Datos Personales.

Los recursos que se interpongan contra la resolución judicial que hiciere lugar a la clausura, no tendrán efecto suspensivo.

Para hacer cumplir dicha resolución, la Unidad Reguladora y Control de Datos Personales podrá requerir el auxilio de la fuerza pública.

La competencia de los Tribunales actuantes se determinará por las normas de la Ley Orgánica de la Judicatura N° 15.750, de 24 de junio de 1985, sus modificativas y concordantes.

Las resoluciones firmes de la Unidad Reguladora y Control de Datos Personales que impongan sanciones pecuniarias, constituyen título ejecutivo.

El monto de las multas previstas en el numeral 3) del presente artículo beneficiará por partes iguales a el o los afectados por la conducta ilegítima y a la Administración.

A tales efectos, la resolución que aplica la multa determinará la suma exacta que la persona física o jurídica infractora deberá pagar a el o los afectados, indicando el domicilio de los mismos y vías de comunicación posibles para que el pago sea efectuado.

El monto destinado a la Administración será recaudado por AGESIC y la totalidad de lo producido por su cobro se verterá a Rentas Generales".

Montevideo, 13 de abril de 2023

MARIANO TUCCI MONTES DE OCA
REPRESENTANTE POR MONTEVIDEO
NICOLÁS VIERA DÍAZ
REPRESENTANTE POR COLONIA
GABRIELA BARREIRO
REPRESENTANTE POR MONTEVIDEO
CARLOS REUTOR
REPRESENTANTE POR CANELONES
LUCÍA ETCHEVERRY LIMA
REPRESENTANTE POR CANELONES
SYLVIA IBARGUREN GAUTHIER
REPRESENTANTE POR RÍO NEGRO
ANA MARÍA OLIVERA PESSANO
REPRESENTANTE POR MONTEVIDEO
NELSON LARZÁBAL NEVES
REPRESENTANTE POR CANELONES
DANIEL GERHARD
REPRESENTANTE POR MONTEVIDEO
DAYANA PÉREZ
REPRESENTANTE POR MONTEVIDEO
CARLOS VARELA NESTIER
REPRESENTANTE POR MONTEVIDEO
ERNESTO GABRIEL OTERO AGÜERO
REPRESENTANTE POR MONTEVIDEO
EDUARDO ANTONINI
REPRESENTANTE POR MALDONADO
LUIS ALFREDO FRATTI
REPRESENTANTE POR CERRO LARGO

_____

EXPOSICIÓN DE MOTIVOS

El presente proyecto de ley está destinado a regular la seguridad digital en el territorio nacional.

Existe acuerdo en el sistema político sobre la necesidad de instituir un marco normativo para que las y los ciudadanos accedan libremente a un recurso fundamental que debe estar reglado, porque los avances tecnológicos en las últimas décadas, han provocado cambios profundos que afectan a las sociedades y naturalmente, a las interacciones entre los individuos.

Por tanto, como es tradición en nuestro país, la legislación debe acompañar los cambios que impone la modernidad, generando obligaciones y garantías para el libre desempeño ciudadano en la utilización de las tecnologías.

En este sentido, frecuentemente nos encontramos en la vida cotidiana con el uso permanente de dispositivos informáticos y espacios virtuales para diversidad de tareas destacando entre ellas, la recreación, el acceso a la información, la comunicación, la educación y el trabajo.

La tarea legislativa debe ofrecer mecanismos de facilitación para el acceso responsable al ciberespacio en sus diferentes modalidades, minimizando las amenazas o los riesgos y respetando los derechos fundamentales de las personas en clave de defensa de las garantías de los sistemas democráticos.

Atentos a estas situaciones, consideramos que tanto los avances tecnológicos y los cambios en las dinámicas sociales, hacen necesaria la revisión de la legislación vigente, no con el cometido exclusivo de agregar o modificar normativa penal, sino fundamentalmente, elaborando un marco normativo que proteja, a través de una regulación garantista de la cual el país carece, aquellas prácticas que son inocuas o incluso deseables.

Asimismo, se hace necesario regular los derechos y responsabilidades, tanto de individuos como de empresas e instituciones cuyas relaciones con las y los ciudadanos están mediadas por la tecnología.

Las normativas sobre seguridad digital deben tener como principal objetivo, garantizar los derechos humanos, aportando al adecuado equilibrio entre el orden y la seguridad pública con los derechos a la libertad de expresión y a la privacidad.

En ese sentido, las regulaciones y políticas a adoptarse deben basarse en evidencias que incluyan el análisis de riesgos y de impacto. La regulación y las medidas a adoptar deben, por lo tanto, garantizar que se establecerán mecanismos que protejan las libertades y derechos, así como la crítica social y política.

Este proyecto trata de abordar los cambios sociales provocados por el aumento virtuoso en el uso de las tecnologías de la información y el conocimiento, incrementada aún más luego de la pandemia de COVID 19.

Muchas de las conductas delictivas que atentan contra la seguridad digital, atacan bienes jurídicos tradicionales mediante la utilización de nuevas tecnologías, lo que se denominan ciberdelitos "en sentido amplio", por lo que resulta suficiente la modificación de los tipos penales ya consagrados en la normativa.

A modo de ejemplo, una persona puede ejercer violencia privada contra otra, ya sea por medios "tradicionales" o mediante tecnologías de la información y comunicación, lo

que no amerita la creación de un tipo penal autónomo, como fue indicado en la comparecencia del Instituto de Derecho Penal y Criminología de nuestra máxima casa de estudios.

Existen otra gama de conductas en donde las tecnologías de la comunicación y de la información resultan el medio y el objetivo de la conducta criminal; son delitos que solamente existen luego del surgimiento de Internet. Para esas conductas se hace necesaria la creación de nuevos tipos penales inexistentes en el catálogo de delitos "tradicionales".

Un marco normativo preciso sobre delitos contra la seguridad digital, mejora la persecución penal de las conductas perjudiciales en la sociedad, promueve una cultura de seguridad y protección en línea, y también contribuye a que empresas y organizaciones tomen medidas adecuadas para proteger sus sistemas y datos de los usuarios.

Sabido es que la mera creación de nuevas tipificaciones penales ha demostrado que por sí sola no colabora con la disminución de las conductas delictivas que han ido en aumento en la misma medida que se han incrementado los guarismos de las penas. Tampoco han mejorado las cifras de éxito en la persecución penal con la creación de tipos y aumentos de penas, por lo que este proyecto intenta vías complementarias para el abordaje de esas prácticas perjudiciales.

Los delitos informáticos son una preocupación actual de la ciudadanía, pero no debe soslayarse la naturaleza de "última ratio" del derecho penal, teniendo presente que el Estado debe reservar la punición penal a lo estrictamente necesario, ya que en materia de criminalidad digital existen medidas más efectivas para la protección de los derechos de los ciudadanos y las ciudadanas, como medios de prevención en seguridad informática y reparación de las víctimas, entre otros.

Asimismo, no solo se deben atacar las conductas delictivas sino que al mismo tiempo se debe garantizar la protección de la libertad de opinión y expresión, así como debe actuarse en pos de la reparación económica de las víctimas en caso de reconocerse la responsabilidad de los encargados de los sistemas de seguridad deficientes que existen en empresas, organismos e instituciones públicas y privadas.

Sin perjuicio de ello, al momento de legislar en materia penal, el legislador se encuentra obligado a dar cumplimiento al principio de legalidad y estricta legalidad, debe establecer los tipos penales de forma precisa, clara y acotada, a la vez que protege la privacidad, el derecho a la libertad de expresión y las tareas que realizan los investigadores en seguridad y vulnerabilidades, así como el respeto de la proporcionalidad de las penas.

Es por todo ello que el presente proyecto aborda modalidades no penales de reparación a las víctimas de los delitos digitales en sede administrativa, ya que la creación de tipos penales no repara pecuniariamente de por sí a la víctima. También se indica que el consumidor tiene derecho a la disposición de los dispositivos propios y a recibir la información necesaria para su modificación o reparación (el "derecho a reparar").

Se explicitan derechos derivados de los preceptos constitucionales como ser el derecho a la investigación académica y a las acciones de identificación de vulnerabilidades de seguridad.

Se establece la obligación de la formación y educación en seguridad digital y la equidad en el acceso y seguridad digital para mujeres y hombres y se regulan potestades

de los clientes respecto a las transacciones bancarias y obligaciones de las entidades financieras para la protección de su seguridad digital.

En el capítulo penal, se consagran algunos delitos digitales específicos a los efectos de tipificar, de la forma más ajustada posible, los accesos ilegítimos a la información en soporte digital, los daños informáticos así como la "estafa" digital y la violencia privada ejercida mediante tecnologías de la información y la comunicación.

Es por lo expuesto anteriormente que ponemos a consideración, la aprobación de este proyecto de ley, ya que el fortalecimiento en la confianza en el entorno digital construye ciudadanía y fortalece relaciones seguras y accesibles y disminuye el riesgo a las vulneraciones de los derechos fundamentales de las personas.

Articulado

Como ya fue expresado, este proyecto de ley busca actualizar la normativa en materia de seguridad digital pero, a su vez, garantizar el ejercicio de los derechos fundamentales de los ciudadanos y las ciudadanas así como encontrar mecanismos que brinden reparación a las víctimas de los delitos definidos en el presente proyecto.

En ese sentido es que el artículo 1º define la finalidad del proyecto de ley, en cuanto a brindar garantías para el uso libre y responsable de las tecnologías de la información y la comunicación, así como definir responsabilidades a quienes abusan con fines maliciosos de estas tecnologías.

Para evitar la amplitud en la normativa, en el artículo 2° se establecen definiciones legales que dan el marco a la normativa propuesta.

El Capítulo I refiere a formas de reparación efectiva a las víctimas, ya que el artículo 3° establece una sanción pecuniaria a imponer en la sentencia de condena de los delitos cometidos mediante tecnologías de información y la comunicación, junto con la pena de privación de libertad, siguiendo el mismo modelo que adoptaron otras leyes en nuestro país.

El artículo 4° establece que el destino de las multas que impone la autoridad monetaria por el incumplimiento de las obligaciones de los emisores de instrumentos electrónicos, será la víctima de dichas fallas de seguridad, generando así una forma de legislar de poco uso en nuestro derecho, como existe en el caso de las denuncias que efectúa el trabajador ante el Banco de Previsión Social.

El artículo 21 establece una solución similar para el destino de las multas que se imponen en base a la Ley N° 18.331 para el caso de incumplimiento en el tratamiento y custodia de los datos personales.

El Capítulo II en el artículo 5° presenta una salvaguarda que establece que debe notificarse previamente al cliente a la realización de una transferencia bancaria, pero el cliente podrá solicitar a la entidad financiera, en caso de no querer recibir dicha notificación previa. El costo del procedimiento no será trasladable al cliente.

El artículo 6° establece la obligatoriedad de que las entidades financieras cuenten con un seguro de responsabilidad o garantía equivalente para el caso en que sean responsables por las fallas de seguridad de sus sistemas.

Los artículos 7° y 8° establecen responsabilidades civiles y administrativas de las entidades financieras que son parte del sistema general de responsabilidad.

El artículo 9° es el único que conforma el Capítulo III y se enmarca en la investigación y acciones de identificación de vulnerabilidades de seguridad, por lo que el legislador entiende necesario protegerlas y así distinguirlas de las actividades con fines delictivos.

Como ya mencionamos, entendemos que las políticas vinculadas a la educación y la igualdad y equidad de accesibilidad y de género son sustanciales tanto para el conocimiento de las tecnologías de la información y la comunicación como para el buen saber de su uso, y así proteger de las posibles vulneraciones de derechos que ocurren en esta moderna modalidad. Es por eso que destinamos el Capítulo IV y los artículos 10 y 11 para regular la formación y promoción en educación así como la equidad e igualdad en el acceso a la seguridad digital.

El Capítulo V incluye regulaciones penales, bajo el principio de que no se trata de nuevas conductas delictivas sino que son otras modalidades de las mismas conductas criminales ya existentes (los artículos 12 a 15), se consagra la agravante del delito si el uso de las nuevas tecnologías ha generado una mayor dañosidad al bien jurídico (artículo 16) y consagra la responsabilidad de la persona física por el no cumplimiento de las normas de seguridad digital previstas en la normativa, lo que es un delito de peligro concreto (artículo 17). El artículo 18 establece la exención de responsabilidad a la persona que obtiene información por medio de las tecnologías de la información y la comunicación o difunde contenidos de interés general, lo que es una solución idéntica a la adoptada por la ley de Prensa.

Los artículos finales (del 19 al 21), enmarcados en el Capítulo VI son disposiciones generales actualizando la normativa al incluir que los datos en soporte digital deben llevar el mismo tratamiento previsto por la Ley de Datos Personales Nº 18.331, así como se establece como derecho del consumidor el acceso a la documentación técnica de los componentes físicos y de software a los efectos de permitir una correcta reparación de los dispositivos.

Entendemos que el cuerpo de este proyecto de ley es integral, abarcativo, garantista de la seguridad digital de las y los ciudadanos y ciudadanas.

Montevideo, 13 de abril de 2023

MARIANO TUCCI MONTES DE OCA
REPRESENTANTE POR MONTEVIDEO
NICOLÁS VIERA DÍAZ
REPRESENTANTE POR COLONIA
GABRIELA BARREIRO
REPRESENTANTE POR MONTEVIDEO
CARLOS REUTOR
REPRESENTANTE POR CANELONES
LUCÍA ETCHEVERRY LIMA
REPRESENTANTE POR CANELONES
SYLVIA IBARGUREN GAUTHIER
REPRESENTANTE POR RÍO NEGRO
ANA MARÍA OLIVERA PESSANO
REPRESENTANTE POR MONTEVIDEO
NELSON LARZÁBAL NEVES
REPRESENTANTE POR CANELONES

DANIEL GERHARD
REPRESENTANTE POR MONTEVIDEO
DAYANA PÉREZ
REPRESENTANTE POR MONTEVIDEO
CARLOS VARELA NESTIER
REPRESENTANTE POR MONTEVIDEO
ERNESTO GABRIEL OTERO AGÜERO
REPRESENTANTE POR MONTEVIDEO
EDUARDO ANTONINI
REPRESENTANTE POR MALDONADO
LUIS ALFREDO FRATTI
REPRESENTANTE POR CERRO LARGO

=/=